



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

CERTIFIED COPY OF
PRIORITY DOCUMENT

出 願 年 月 日
Date of Application:

1999年 3月15日

出 願 番 号
Application Number:

平成11年特許願第069152号

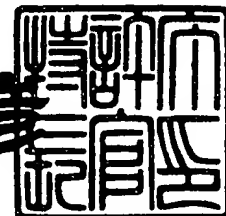
出 願 人
Applicant (s):

ソニー株式会社

2000年 1月21日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特平11-3095140

【書類名】 特許願

【整理番号】 9900143603

【提出日】 平成11年 3月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 大石 丈於

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 岡上 拓己

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100094053

 【弁理士】

 【氏名又は名称】 佐藤 隆久

【手数料の表示】

 【予納台帳番号】 014890

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9707389

特平 1 1 - 0 6 9 1 5 2

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置、データ処理システムおよびその方法

【特許請求の範囲】

【請求項 1】

所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、

前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、

前記暗号化したデータを記憶する記憶手段と、

同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す制御手段と

を有するデータ処理装置。

【請求項 2】

前記制御手段は、前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する

請求項 1 に記載のデータ処理装置。

【請求項 3】

前記暗号化手段は、前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化する

請求項 1 に記載のデータ処理装置。

【請求項 4】

前記制御手段は、単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶手段に記憶された前記暗号化されたデータを管理する

請求項 3 に記載のデータ処理装置。

【請求項 5】

前記制御手段は、前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する

請求項 4 に記載のデータ処理装置。

【請求項 6】

前記制御手段は、前記処理ブロック単位で読み出した前記データを前記処理手段に出力する

請求項 1 に記載のデータ処理装置。

【請求項 7】

前記データは圧縮されており、

前記処理手段は、前記記憶手段から読み出された前記データを、前記処理ブロックを単位として伸長する

請求項 6 に記載のデータ処理装置。

【請求項 8】

記憶装置とデータ処理装置との間で相互認証を行いながらデータの入出力を行うデータ処理システムにおいて、

前記記憶装置は、

前記データ処理装置との間で相互認証処理を行う第 1 の相互認証処理手段と、
前記データを記憶する記憶手段と、

前記相互認証処理によって前記データ処理装置が正当な相手であると認めるときに、前記データ処理装置と前記記憶手段との間でデータの入出力を行わせる第 1 の制御手段と

を有し、

前記データ処理装置は、

前記記憶装置との間で相互認証処理を行う第 2 の相互認証処理手段と、

所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、

前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、

前記相互認証処理によって前記記憶装置が正当な相手であると認めたときに、書き込み処理および読み出し処理のうち少なくとも一方を行う、前記書き込み処理において、同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記記憶手段に書き込み、前記読み出し処理において、前記処理ブロックを単位として前記データを前記記憶手段から読み出す第 2 の制御手段と

を有する

データ処理システム。

【請求項 9】

前記第 2 の制御手段は、前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する

請求項 8 に記載のデータ処理システム。

【請求項 1 0】

前記暗号化手段は、前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化する

請求項 8 に記載のデータ処理システム。

【請求項 1 1】

前記第 2 の制御手段は、単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶手段に記憶された前記暗号化されたデータを管理する

請求項 1 0 に記載のデータ処理システム。

【請求項 1 2】

前記第 2 の制御手段は、前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する

請求項 1 1 に記載のデータ処理システム。

【請求項 1 3】

所定のデータ長の暗号化ブロックを単位としてデータを暗号化し、

前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行い、

同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す

データ処理方法。

【請求項 1 4】

前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する

請求項 1 3 に記載のデータ処理方法。

【請求項 1 5】

前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化して前記暗号化を行う

請求項 1 3 に記載のデータ処理方法。

【請求項 1 6】

単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶

手段に記憶された前記暗号化されたデータを管理する

請求項 1 5 に記載のデータ処理方法。

【請求項 1 7】

前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する

請求項 1 6 に記載のデータ処理方法。

【請求項 1 8】

前記記憶手段から読み出された前記データを、前記処理ブロックを単位として伸長する

請求項 1 3 に記載のデータ処理方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶手段に記憶するデータ処理装置、データ処理システムおよびその方法に関する。

【0 0 0 2】

【従来の技術】

例えば、著作権侵害となる不正利用を防止するために、オーディオデータなどのデータを、所定のデータ長の暗号化ブロックを単位として暗号化して記憶媒体に記憶することがある。

この場合に、暗号化しようとするデータは、通常、所定の圧縮処理ブロックを単位として圧縮されていることが多い。

【0003】

【発明が解決しようとする課題】

ところで、上述したように圧縮されたデータを暗号化して記録媒体に記録する場合に、圧縮ブロックと暗号化ブロックとは通常一致しない。

そのため、例えば、圧縮ブロックを単位として記録媒体からデータを読み出すと、暗号化ブロックのうち一部のデータが読み出されないことがあり、正確な復号を行えなくなる。このような事態を回避するため、圧縮ブロックおよび暗号ブロックの双方を考慮して読み出しを行うと、処理が煩雑になるとう問題がある。

【0004】

また、記録媒体に記録したデータを編集する場合などは、例えば圧縮ブロックを単位としてデータの分割および結合などが行われるが、この場合にも、編集後のデータに暗号化ブロックの一部のデータが含まれなくなる可能性が高く、同様に、正確な復号が行えなくなるという問題がある。

また、圧縮されていないデータであっても、例えば、音楽用のCD (Compact Disk) フォーマットなどのように、所定のブロックを単位として処理が行われる場合にも上述した場合と同様の問題が生じる。

【0005】

本発明は上述した従来技術の問題点に鑑みてなされ、例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶媒体に記憶する際に、所定の処理ブロックに基づいた処理と復号処理とを簡単な構成で正確に行うことができるデータ処理装置、データ処理システムおよびその方法を提供することを目的とする。

【0006】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第1の観点のデータ処理装置は、所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、前記暗号化したデータを記憶する記憶手段と、同じ前記暗号化ブロック内に位置するデー

タが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す制御手段とを有する。

【0007】

また、本発明のデータ処理装置は、好ましくは、前記制御手段は、前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する。

【0008】

また、本発明のデータ処理装置は、好ましくは、前記暗号化手段は、前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化する。

【0009】

また、本発明のデータ処理装置は、好ましくは、前記制御手段は、単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶手段に記憶された前記暗号化されたデータを管理する。

【0010】

また、本発明のデータ処理装置は、好ましくは、前記制御手段は、前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する。

【0011】

また、本発明のデータ処理システムは、記憶装置とデータ処理装置との間で相互認証を行いながらデータの入出力を行うデータ処理システムであって、前記記憶装置は、前記データ処理装置との間で相互認証処理を行う第1の相互認証処理

手段と、前記データを記憶する記憶手段と、前記相互認証処理によって前記データ処理装置が正当な相手であると認めたときに、前記データ処理装置と前記記憶手段との間でデータの入出力を行わせる第1の制御手段とを有する。また、前記データ処理装置は、前記記憶装置との間で相互認証処理を行う第2の相互認証処理手段と、所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、前記相互認証処理によって前記記憶装置が正当な相手であると認めたときに、書き込み処理および読み出し処理のうち少なくとも一方を行う、前記書き込み処理において、同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記記憶手段に書き込み、前記読み出し処理において、前記処理ブロックを単位として前記データを前記記憶手段から読み出す第2の制御手段とを有する。

【0012】

さらに、本発明のデータ処理方法は、所定のデータ長の暗号化ブロックを単位としてデータを暗号化し、前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行い、同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す。

【0013】

【発明の実施の形態】

以下、本発明の実施形態に係わるオーディオシステムについて説明する。

図1は本実施形態のオーディオシステム1のシステム構成図、図2は図1に示す携帯用記憶装置3および携帯用プレーヤ4の内部構成図である。

図1に示すように、オーディオシステム1は、例えば、コンピュータ2、携帯用記憶装置3、携帯用プレーヤ4、CD-ROMドライブ6およびCDプレーヤ7を有する。

【0014】

コンピュータ 2

コンピュータ 2 は、ネットワーク 5 に接続されており、例えば、EMD (Electronic Music Distribution: 電子音楽配信) などのサービスを提供する図示しないサービスプロバイダのホストコンピュータから、ネットワーク 5 を介してオーディオデータ（トラックデータ）を受信し、当該受信したオーディオデータを必要に応じて復号して、携帯用プレーヤ 4 に出力する。

また、コンピュータ 2 は、コンテンツデータを受信するに当たって、必要に応じて、サービスプロバイダのホストコンピュータとの間で認証処理および課金処理などを行う。

また、コンピュータ 2 は、例えば、CD-ROM ドライブ 6 から入力したオーディオデータを携帯用プレーヤ 4 に出力する。

【0015】

携帯用記憶装置 3

携帯用記憶装置 3 は、例えば、メモリスティックであり、フラッシュメモリなどの書き換え可能な半導体メモリを内蔵している。

図 2 に示すように、携帯用記憶装置 3 は、例えば、主制御モジュール 31、通信インタフェース 32、制御モジュール 33、フラッシュメモリ 34 およびフラッシュメモリ管理モジュール 35 を有する。

【0016】

〔制御モジュール 33〕

図 2 に示すように、制御モジュール 33 は、例えば、乱数発生ユニット 50、記憶ユニット 51、鍵生成／演算ユニット 52、相互認証ユニット 53、暗号化／復号ユニット 54 および制御ユニット 55 を有する。

制御モジュール 33 は、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール 33 は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。

乱数発生ユニット 50 は、乱数発生指示を受けると、64 ビット（8 バイト）

の乱数を発生する。

【0017】

記憶ユニット51は、例えば、EEPROM(Electrically Erasable Programmable Read Only Memory)などの不揮発性メモリであり、認証処理に必要な鍵データなどの種々のデータを記憶している。

図3は、記憶ユニット51に記憶されているデータを説明するための図である。

図3に示すように、記憶ユニット51は、認証鍵データ $IK_0 \sim IK_{31}$ 、装置識別データ ID_m および記憶用鍵データ SK_m を記憶している。

認証鍵データ $IK_0 \sim IK_{31}$ は、携帯用記憶装置3が携帯用プレーヤ4との間で相互認証を行う際に用いられる鍵データであり、後述するように相互認証を行う度に認証鍵データ $IK_0 \sim IK_{31}$ のうちの認証鍵データがランダムに選択される。なお、認証鍵データ $IK_0 \sim IK_{31}$ および記憶用鍵データ SK_m は、携帯用記憶装置3の外部から読めないようになっている。

装置識別データ ID_m は、携帯用記憶装置3に対してユニークに付けられた識別データであり、後述するように、携帯用記憶装置3が携帯用プレーヤ4との間で相互認証を行う際に読み出されて携帯用プレーヤ4に出力される。

記憶用鍵データ SK_m は、後述するように、トラック鍵データ TRK を暗号化してフラッシュメモリ34に記憶する際に用いられる。

【0018】

鍵生成/演算ユニット52は、例えば、ISO/IEC9797のMAC(Message Authentication Code)演算などの種々の演算を行って鍵データを生成する。このとき、MAC演算には、例えば、“Block cipher Algorithm”としてFIPS PUB 46-2に規定されるDES(Data Encryption Standard)が用いられる。

MAC演算は、任意の長さのデータを固定の長さに圧縮する一方向性ハッシュ関数演算であり、関数値が秘密鍵に依存して定まる。

【0019】

相互認証ユニット53は、携帯用プレーヤ4からオーディオデータを入力して

フラッシュメモリ 34 に書き込む動作を行うのに先立って、携帯用プレーヤ 4 との間で相互認証処理を行う。

また、相互認証ユニット 53 は、フラッシュメモリ 34 からオーディオデータを読み出して携帯用プレーヤ 4 に出力する動作を行うのに先立って、携帯用プレーヤ 4 との間で相互認証処理を行う。

また、相互認証ユニット 53 は、相互認証処理において、前述した MAC 演算を行う。

当該相互認証処理では、記憶ユニット 51 に記憶されているデータが用いられる。

【0020】

暗号化／復号ユニット 54 は、DES、IDEA、MISTY などのブロック暗号アルゴリズムでの暗号化を行う。使用するモードは、FIPS PUB 81 "DES MODES OF OPERATION" に規定されているような ECB (Electronic Code Book) モードおよび CBC (Cipher Block Chaining) モードである。

また、暗号化／復号ユニット 54 は、DES、IDEA、MISTY などのブロック復号アルゴリズムでの復号を行う。使用するモードは、上記 ECB モードおよび CBC モードである。

当該 ECB モードおよび CBC モードのブロック暗号化／復号では、指定された鍵データを用いて指定されたデータを暗号化／復号する。

制御ユニット 55 は、乱数発生ユニット 50、記憶ユニット 51、鍵生成／演算ユニット 52、相互認証ユニット 53 および暗号化／復号ユニット 54 の処理を統括して制御する。

【0021】

〔フラッシュメモリ 34〕

フラッシュメモリ 34 は、例えば、32M バイトの記憶容量を有する。

フラッシュメモリ 34 には、相互認証ユニット 53 による相互認証処理によって正当な相手であると認められたときに、携帯用プレーヤ 4 から入力したオーディオデータが書き込まれる。

また、フラッシュメモリ 34 からは、相互認証ユニット 53 による相互認証処理によって正当な相手であると認められたときに、オーディオデータが読み出されて携帯用プレーヤ 4 に出力される。

以下、フラッシュメモリ 34 に記憶されるデータおよびそのフォーマットについて説明する。

図 4 は、フラッシュメモリ 34 に記憶されるデータを説明するための図である。

図 4 に示すように、フラッシュメモリ 34 には、例えば、トラック管理ファイル 100、トラックデータファイル 101₀、101₁、101₂、101₃ が記憶されている。

ここで、トラック管理ファイル 100 はトラックデータファイル 101₀ ~ 101₃ を管理する管理データを有し、トラックデータファイル 101₀ ~ 101₃ はそれぞれ対応するトラックデータ（オーディオデータ）を有している。

なお、本実施形態では、トラックデータは、例えば、1 曲分のオーディオデータを意味する。

【0022】

図 5 は、トラック管理ファイル 100 のフォーマットを説明するための図である。

図 5 に示すように、トラック管理ファイル 100 は、トラックデータ（楽曲）毎の管理情報を記述した管理データ TRKINF (0)、TRKINF (1)、TRKINF (2)、TRKINF (3) と、トラックデータ毎のパーツ情報を記述した管理データ PRTINF (0)、PRTINF (1)、PRTINF (2)、PRTINF (3) とを有している。

ここで、管理データ TRKINF (0) および PRTINF (0) は、図 4 に示すトラックデータファイル 101₀ の管理データである。

管理データ TRKINF (1) および PRTINF (1) は、図 4 に示すトラックデータファイル 101₁ の管理データである。

管理データ TRKINF (2) および PRTINF (2) は、図 4 に示すトラックデータファイル 101₂ の管理データである。

管理データ $TRKINF(3)$ および $PRTINF(3)$ は、図4に示すトラックデータファイル 101_3 の管理データである。

【0023】

ここで、 n を $0 \leq n \leq 3$ の整数とした場合に、管理データ $TRKINF(n)$ は、図6に示すように、 FNM 、 TRK 、 $S-SAMSERIAL$ 、 $CONNUM$ 、 P 、 $PNM1(OP)$ を有している。

【0024】

ここで、 FNM は、トラックデータファイル 100_n の名前を示している。

TRK は、暗号化されたトラック鍵データ TRK を示している。

$S-SAMSERIAL$ は、図2に示す制御モジュール43のシリアル番号を示している。

また、 $CONNUM$ は、同一の $S-SAMSERIAL$ 番号内で重複しないように、トラックデータファイル毎にユニークに付けられたトラック累積番号を示している。

P は、トラックデータを構成するパーツ数を示している。なお、本実施形態では、パーツとは、録音開始から停止までの連続した時間内で記録されたデータの単位を示しており、通常、1トラックデータは1パーツで構成される。但し、後述するように、結合編集処理が行われると、1トラックデータに複数のパーツが含まれる場合がある。

$PNM1(OP)$ は、曲名ファイルへのポインタを示している。

【0025】

また、管理データ $PRTINF(n)$ は、圧縮モードなどの属性、パーツサイズなどの情報を示しており、図6に示すように、パーツ毎に $PRTSIZE$ および PK を有している。

図6に示す例では、管理データ $PRTINF(n)$ が管理するトラックデータ内に、 $(m+1)$ 個のパーツが含まれる場合を例示している。

ここで、 $PRTSIZE(0) \sim (m)$ は、それぞれ対応するパーツのクラスサイズ、当該パーツの始まりとなるサウンドユニット SU およびパーツの終わりとなるサウンドユニット SU を特定する情報を示している。

PK (0) ~ (m) は、それぞれ対応するパーツのオーディオデータを暗号化するのに用いるクラスタ鍵データ CK を生成する際に、トラック鍵データ TRK と共に用いられるパーツ鍵データ PK を示している。パーツ鍵データ PK は、パーツ毎に生成される。

【0026】

以下、トラックデータファイル 101₀ ~ 101₃ について説明する。

図 7 は、トラックデータファイル 101₀ の構成を説明するための図である。

図 7 に示すように、トラックデータファイル 101₀ は、1 個のパーツからなり、当該パーツが 5 個のクラスタ CL (0), CL (1), CL (2), CL (3), CL (4) で構成されている。当該パーツは、クラスタ CL (0) の先頭から開始し、クラスタ CL (4) のサウンドユニット SU (4) で終了している。

なお、トラックデータファイル 101₁ ~ 101₃ は、基本的に、図 7 に示す構成をしているが、パーツ数、クラスタ数およびクラスタ内に含まれるサウンドユニット SU の数は、図 7 に示すものには限定されず、独立して決められている。

【0027】

図 8 は、クラスタ CL の構成を説明するための図である。

図 8 に示すように、クラスタ CL は、連続したアドレスに順次に記憶された 8 バイトのブロック暗号化初期値 IV、例えば、各々 160 バイトのサウンドユニット SU (0) ~ (101) およびクラスタシードデータ CS を有する。

すなわち、ブロック暗号化初期値 IV が、サウンドユニット SU (0) の直前のアドレスに記憶されている。

ここで、ブロック暗号化初期値 IV は、後述するように、図 2 に示す暗号化／復号ユニット 64 における CBC モードの暗号化および復号に用いられる。

【0028】

また、サウンドユニット SU (0) ~ (101) は、図 2 に示す暗号化／復号ユニット 64 において CBC (Cipher Block Chaining) モードで 64 ビット (8 バイト) の暗号化ブロックを単位として暗号化して生成された 8 バイトの暗号文

C_i によって構成される。

本実施形態では、サウンドユニット SU のバイト数（例えば 160 バイト）を、暗号化の単位である暗号化ブロックのバイト数（例えば 8 バイト）の整数倍にしている。

すなわち、1 サウンドユニット SU は例えば 20 個の暗号文 C_i からなる。

このとき、個々の暗号文 C_i は一のサウンドユニット SU 内に位置し、一の暗号文 C_i が複数のサウンドユニット SU に跨がって位置することはない。

ここで、フラッシュメモリ 34 に記憶されているオーディオデータは、後述するように例えば、ATRAC3 方式で圧縮されており、当該圧縮の単位がサウンドユニット SU である。従って、携帯用記憶装置 3 から携帯用プレーヤ 4 にオーディオデータを読み出す場合には、読み出しの最小単位は当該サウンドユニット SU となる。

このようにすることで、フラッシュメモリ 34 に記憶されている暗号化されたオーディオデータにアクセスする際に、暗号化ブロックの区切りを意識する必要がなくなり、当該アクセスに伴う処理負担を軽減できる。

なお、各クラスタ内に含まれるサウンドユニット SU の数は、1 個以上 102 個以下の範囲で任意である。

また、オーディオデータの圧縮方式は、ATRAC3 などの ATRAC 方式以外の CODEC 方式でもよい。

クラスタシードデータ CS は、各クラスタ毎に例えば乱数を発生して生成されたデータであり、後述するように、携帯用プレーヤ 4 内でクラスタ毎にクラスタ鍵データ CK を生成する際に用いられる。

当該クラスタシードデータ CS は、エラー対策としてクラスタ内の 2 箇所に格納されている。

【0029】

〔フラッシュメモリ管理モジュール 35〕

フラッシュメモリ管理モジュール 35 は、フラッシュメモリ 34 へのデータの書き込み、フラッシュメモリ 34 からのデータの読み出しなどの制御を行う。

【0030】

携帯用プレーヤ4

図2に示すように、携帯用プレーヤ4は、例えば、主制御モジュール41、通信インタフェース42、制御モジュール43、編集モジュール44、圧縮／伸長モジュール45、スピーカ46、D／A変換器47およびA／D変換器48を有する。

【0031】

〔主制御モジュール41〕

主制御モジュール41は、携帯用プレーヤ4の処理を統括的に制御する。

〔制御モジュール43〕

図2に示すように、制御モジュール43は、例えば、乱数発生ユニット60、記憶ユニット61、鍵生成／鍵演算ユニット62、相互認証ユニット63、暗号化／復号ユニット64および制御ユニット65を有する。

制御モジュール43は、制御モジュール33と同様に、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール43は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパ性を有している。

乱数発生ユニット60は、乱数発生指示を受けると、64ビット（8バイト）の乱数を発生する。

記憶ユニット61は、認証処理に必要な種々のデータを記憶している。

図9は、記憶ユニット61に記憶されているデータを説明するための図である。

図9に示すように、記憶ユニット61は、マスター鍵データ $MK_0 \sim MK_{31}$ および装置識別データ ID_d を記憶している。

ここで、マスター鍵データ $MK_0 \sim MK_{31}$ と、認証鍵データ $IK_0 \sim IK_{31}$ の間には、前述した携帯用記憶装置3の装置識別データ ID_m を用いて、下記式（1）に示す関係がある。

なお、下記式において、 $f(a, b)$ は、例えば、引数 a, b から値を導出す

る関数である。

【0032】

【数1】

$$IK_j = f(MK_j, ID_m) \quad \dots (1)$$

但し、 i は、 $0 \leq j \leq 31$ の整数。

【0033】

また、記憶ユニット61における認証鍵データ $IK_0 \sim IK_{31}$ の記憶アドレスは、例えば5ビットで表現され、それぞれ記憶ユニット51におけるマスター鍵データ $MK_0 \sim MK_{31}$ と同じ記憶アドレスが割り当てられている。

【0034】

鍵生成／鍵演算ユニット62は、例えば、ISO/IEC 9797のMAC演算方式を用いた演算などの種々の演算を行って鍵データを生成する。このとき、“Block cipher Algorithm”としてFIPS PUB 46-2に規定されるDESが用いられる。

【0035】

相互認証ユニット63は、例えば、コンピュータ2から入力したオーディオデータを携帯用記憶装置3に出力する動作を行うのに先立って、携帯用記憶装置3との間で相互認証処理を行う。

また、相互認証ユニット63は、携帯用記憶装置3からオーディオデータを入力する動作を行うのに先立って、携帯用記憶装置3との間で相互認証処理を行う。

また、相互認証ユニット63は、相互認証処理において、前述したMAC演算を行う。

当該相互認証処理では、記憶ユニット61に記憶されているデータが用いられる。

なお、相互認証ユニット63は、必要に応じて、例えば、コンピュータ2あるいはネットワーク5上のコンピュータとの間でオーディオデータの入出力を行う動作に先立って、コンピュータ2あるいはネットワーク5上のコンピュータとの間で相互認証処理を行う。

【0036】

暗号化／復号ユニット64は、前述したように、FIPS PUB 81に規定されたECBモードおよびCBCモードを選択的に用いてブロック暗号化を行う。

ここで、暗号化／復号ユニット64は、CBCモードにおいて、56ビットの鍵データkを用いて、コンピュータ2あるいはCDプレーヤ7から入力したオーディオデータ（平文）を、64ビットからなる暗号化ブロックを単位として下記式（2）に基づいて暗号化して暗号化されたオーディオデータ（暗号文）を生成する。

下記式（2）から分かるように、CBCモードでは、一つ前の暗号文と次の平文との排他的論理和を暗号化するため、同一の平文が入力されても異なる暗号文が出力され、解読が困難であるという利点がある。

【0037】

【数2】

$$C_i = E_k (P_i \text{ XOR } C_{i-1}) \quad \dots (2)$$

i : 1以上の整数

P_i : 平文（64ビット）

C_i : 暗号文（64ビット）

XOR : 排他的論理和

E_k : 56ビットの鍵データkを用いたDES方式の暗号処理

【0038】

上記式（2）の演算は、図10で表現される。なお、図10において、「IV」は、ブロック暗号化初期値（64ビット）であり、図2に示す携帯用記憶装置3のフラッシュメモリ34において、図8に示すようにクラスタCL内のサウンドユニットSU（0）の直前に記憶される。

【0039】

なお、コンピュータ2あるいはCDプレーヤ7から入力したオーディオデータ（平文）は、ATRAC (Adaptive Transform Audio Coder)方式を改良したATRAC3方式で圧縮されている。

なお、ATRACは、MD(Mini Disk：商標)のための符号化圧縮方式であり、例えば、288kbit/sで44.1kHzサンプルのステレオ信号が、帯域分割とMDCT(Modified Discrete Cosine Transform)とを併用して符号されている。すなわち、まず、帯域分割フィルタで1/4, 1/4, 1/2の3つの帯域に分割され、それぞれの帯域の信号がダウンサンプルされ、時間領域の信号としてMDCTで周波数領域に変換され、当該MDCTの係数が適応ビット配分を行ってスカラ量子化されている。

【0040】

暗号化／復号ユニット64は、FIPS81のモードのうち、前述したECBモードおよびCBCモードの復号を選択的に行う。

ここで、暗号化／復号ユニット64は、CBCモードにおいて、56ビットの鍵データkを用いて、暗号文を、64ビットからなる暗号化ブロックを単位として下記式(3)に基づいて復号して平文を生成する。

【0041】

【数3】

$$P_i = C_{i-1} \text{ XOR } D_k(C_i) \quad \dots (3)$$

i : 1以上の整数

P_i : 平文(64ビット)

C_i : 暗号文(64ビット)

XOR : 排他的論理和

D_k : 56ビットの鍵データkを用いたDES方式の復号処理

【0042】

上記式(3)の演算は、図11で表現される。なお、図11において、「IV」は、ブロック暗号化初期値(64ビット)であり、図2に示す携帯用記憶装置3のフラッシュメモリ34において図8に示すようにクラスタCL内のサウンドユニットSU(0)の直前に記憶されたものが用いられる。

【0043】

制御ユニット65は、乱数発生ユニット60、記憶ユニット61、鍵生成／鍵演算ユニット62、相互認証ユニット63および暗号化／復号ユニット64の処

理を統括的に制御する。

【0044】

〔編集モジュール44〕

編集モジュール44は、例えば、図4に示すように携帯用記憶装置3のフラッシュメモリ34内に記憶されたトラックデータファイル101₀～101₃を、ユーザからの操作指示に基づいて編集して新たなトラックデータファイルを生成する。

当該編集には、1個のトラックデータファイルを分割して2個のトラックデータファイルを生成する分割編集処理と、2個のトラックデータファイルを結合して1個のトラックデータファイルを生成する結合編集処理とがある。

なお、当該編集にあたって、図5および図6に示すトラック管理ファイル100およびトラックデータファイル101₀～101₃が書き換えられる。

編集モジュール44における編集処理については後に詳細に説明する。

【0045】

〔圧縮／伸長モジュール45〕

圧縮／伸長モジュール45は、例えば、携帯用記憶装置3から入力した暗号化されたオーディオデータを復号した後に再生する際に、ATRAC3方式で圧縮されているオーディオデータを伸長し、当該伸長したオーディオデータをD/A変換器47に出力する。

また、例えば、CDプレーヤ7あるいはコンピュータ2から入力したオーディオデータを、携帯用記憶装置3に記憶する際に、当該オーディオデータをATRAC3方式で圧縮する。

【0046】

〔D/A変換器47〕

D/A変換器47は、圧縮／伸長モジュール45から入力したデジタル形式のオーディオデータをアナログ形式のオーディオデータに変換してスピーカ46に出力する。

〔スピーカ46〕

スピーカ46は、D/A変換器47から入力したオーディオデータに応じた音

響を出力する。

〔A／D変換器 4 8〕

A／D変換器 4 8は、例えば、CDプレーヤ7から入力したアナログ形式のオーディオデータをデジタル形式に変換して圧縮／伸長モジュール4 5に出力する。

【0 0 4 7】

以下、図 1 に示すオーディオシステム 1 の動作について説明する。

携帯用記憶装置 3 への書き込み動作

図 1 2 は、携帯用プレーヤ 4 から携帯用記憶装置 3 への書き込み動作を説明するためのフローチャートである。

ステップ S 1：携帯用プレーヤ 4 から携帯用記憶装置 3 に、書き込み要求信号が出力される。

ステップ S 2：携帯用記憶装置 3 と携帯用プレーヤ 4 との間で、相互認証処理を行う際に用いる認証鍵データ IK_j の選択処理が行われる。当該処理については後述する。

ステップ S 3：携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証処理が行われる。当該処理については後述する。

ステップ S 4：ステップ S 3 の相互認証処理によって携帯用記憶装置 3 および携帯用プレーヤ 4 の双方が相手を正当であると認めた場合には、ステップ S 5 の処理が行われ、そうでない場合には処理が終了する。

ステップ S 5：携帯用記憶装置 3 および携帯用プレーヤ 4 において、セッション鍵データ Se_k が生成される。当該処理については後述する。

ステップ S 6：携帯用プレーヤ 4 から携帯用記憶装置 3 に、通信インタフェース 3 2，4 2 を介して、暗号化したオーディオデータを出力して書き込む。当該処理については後述する。

このように、オーディオシステム 1 によれば、携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、携帯用プレーヤ 4 から携帯用記憶装置 3 に、暗号化されたオーディオデータを書き込まれる。

そのため、著作権侵害を招くようなオーディオデータの不正な複製が容易に行われることを回避できる。

【0048】

〔認証鍵データ IK_j の選択処理（図12に示すステップS2）〕

図13は、認証鍵データ IK_j の選択処理を説明するための図である。

図13に示すように、図2に示す携帯用プレーヤ4の乱数発生ユニット60によって64ビットの乱数 R_j が生成される。

当該乱数 R_j は、携帯用プレーヤ4から携帯用記憶装置3に出力される。

そして、携帯用記憶装置3の相互認証ユニット53によって、64ビットの乱数 R_j の下位5ビットを用いて、記憶ユニット51に記憶されている認証鍵データ $IK_0 \sim IK_{31}$ のうちの認証鍵データ IK_j （ j は $0 \leq j \leq 31$ を満たす整数）が特定される。

また、携帯用記憶装置3の記憶ユニット51から読み出された装置識別データ ID_m が、携帯用記憶装置3から携帯用プレーヤ4に出力される。

そして、携帯用プレーヤ4の相互認証ユニット63によって、乱数 R_j の下位5ビットを用いて、マスター鍵データ $MK_0 \sim MK_{31}$ のうちのマスター鍵データ MK_j が特定される。

そして、鍵生成／鍵演算ユニット62において、前記特定されたマスター鍵データ MK_j と、携帯用記憶装置3から入力した装置識別データ ID_m とを用いて、下記式（4）に基づいて、認証鍵データ IK_j を生成する。

下記式（4）において、 $f(a, b)$ は、例えば、引数 a, b から値を導出する任意の関数である。

【0049】

【数4】

$$IK_j = f(MK_j, ID_m) \quad \dots (4)$$

【0050】

これにより、携帯用記憶装置3と携帯用プレーヤ4とが、上記式（4）に示す関係を持つ認証鍵データ $IK_0 \sim IK_{31}$ およびマスター鍵データ $MK_0 \sim MK_{31}$ を有している場合には、図13に示す処理によって同じ認証鍵データ IK_j が選

択される。

当該選択された認証鍵データ IK_j は、後述する相互認証処理を行う際に、秘密鍵として用いられる。

また、このとき、32個の認証鍵データ IK_j のうち選択される認証鍵データは、図13に示す処理を行う毎に乱数 R_j に応じてランダムに決定される。

そのため、不正な認証が成功する確率を、一の認証鍵データを固定して用いる場合の $1/32$ 倍にすることができ、不正な認証が行われることを高い確率で回避できる。

なお、上述した実施形態では、乱数を用いて8個の認証鍵データ IK_j のうち一の認証鍵データを選択する場合を例示したが、携帯用記憶装置3および携帯用プレーヤ4の外部から入力した鍵指定信号に基づいて選択する認証鍵データを決定してもよい。

【0051】

〔携帯用記憶装置3と携帯用プレーヤ4との間の相互認証処理（図12に示すステップS3）〕

図14は、携帯用記憶装置3と携帯用プレーヤ4との間の相互認証処理を説明するための図である。

なお、当該相互認証処理を開始するときには、前述した図13に示す認証鍵データ IK_j の選択処理が終了しており、携帯用プレーヤ4の相互認証ユニット53は、選択した認証鍵データ IK_j を有している。また、携帯用記憶装置3の相互認証ユニット63は、選択した認証鍵データ IK_j 、携帯用記憶装置3の装置識別データ ID_m を有している。

【0052】

ステップS10：携帯用記憶装置3の乱数発生ユニット50において、64ビットの乱数 R_{ms} を生成し、これを携帯用プレーヤ4に出力する。

ステップS11：携帯用プレーヤ4の乱数発生ユニット60において、64ビットの乱数 R_d および S_d を生成する。

ステップS12：携帯用プレーヤ4の相互認証ユニット63において、図12に示すステップS2で得た認証鍵データ IK_j および「 $R_d \parallel R_{ms} \parallel ID_m$ 」を

用いて、下記式(5)に基づいてMAC演算を行い、 MAC_A を求める。

ここで、 $A \parallel B$ は、AとBの連結(nビットのAの後ろにmビットのBを結合して(n+m)ビットとしたもの)を示す。

【0053】

【数5】

$$MAC_A = MAC(IK_j, R_d \parallel R_{ms} \parallel ID_m) \quad \dots (5)$$

【0054】

ステップS13: 携帯用プレーヤ4は、「 $R_d \parallel S_d \parallel MAC_A \parallel j$ 」を携帯用記憶装置3に出力する。

【0055】

ステップS14: 携帯用記憶装置3の相互認証ユニット53において、図12に示すステップS2で得た認証鍵データ IK_j および「 $R_d \parallel R_{ms} \parallel ID_m$ 」を用いて、下記式(6)に基づいてMAC演算を行い、 MAC_B を求める。

【0056】

【数6】

$$MAC_B = MAC(IK_j, R_d \parallel R_{ms} \parallel ID_m) \quad \dots (6)$$

【0057】

ステップS15: 携帯用記憶装置3の相互認証ユニット53において、ステップS14で求めた MAC_B とステップS13で入力した MAC_A とを比較し、一致していれば、携帯用プレーヤ4が適切な認証鍵データ IK_j を有していることが分かるため、携帯用記憶装置3は携帯用プレーヤ4が正当な相手であると認証する。

【0058】

ステップS16: 携帯用記憶装置3の相互認証ユニット53において、図12に示すステップS2で得た認証鍵データ IK_j および「 $R_{ms} \parallel R_d$ 」を用いて、下記式(7)に基づいてMAC演算を行い、 MAC_C を求める。

【0059】

【数7】

$$MAC_C = MAC(IK_j, R_{ms} \parallel R_d) \quad \dots (7)$$

【0060】

ステップS17：携帯用記憶装置3の乱数発生ユニット50において、64ビットの乱数 S_{ms} を生成する。

【0061】

ステップ18：携帯用記憶装置3から携帯用プレーヤ4に、「 $S_{ms} \parallel MAC_C$ 」を出力する。

【0062】

ステップS19：携帯用プレーヤ4の相互認証ユニット63において下記式（8）に基づいてMAC演算を行い、 MAC_d を求める。

【0063】

【数8】

$$MAC_d = MAC(IK_j, R_{ms} \parallel R_d) \quad \dots (8)$$

【0064】

ステップS20：携帯用プレーヤ4の相互認証ユニット63において、ステップS19で求めた MAC_d とステップS18で入力した MAC_C とを比較し、一致していれば、携帯用記憶装置3が適切な認証鍵データ IK_j を有していることが分かるため、携帯用プレーヤ4は携帯用記憶装置3が正当な相手であると認証する。

以上により、携帯用記憶装置3と携帯用プレーヤ4との間の相互認証が行われる。

【0065】

〔セッション鍵データ Se_k の生成処理（図12に示すステップS5）〕

図15は、セッション鍵データ Se_k の生成処理を説明するための図である。

なお、当該セッション鍵データ Se_k の生成処理を開始するときには、前述した図13に示す認証鍵データ IK_j の選択処理および図14に示す相互認証処理が終了しており、携帯用記憶装置3および携帯用プレーヤ4の双方は、選択した認証鍵データ IK_j および乱数 S_d 、 S_{ms} を有している。

【0066】

ステップS30：携帯用プレーヤ4の相互認証ユニット63は、選択した認証

鍵データ IK_j および「 $S_d \parallel S_{ms}$ 」を用いて、下記式 (9) に基づいて MAC 演算を行い、セッション鍵データ Se_k を生成する。

【0067】

【数9】

$$\text{セッション鍵データ } Se_k = \text{MAC} (IK_j, S_d \parallel S_{ms}) \quad \dots (9)$$

【0068】

ステップ S31：携帯用記憶装置 3 の相互認証ユニット 53 は、選択した認証鍵データ IK_j および「 $S_d \parallel S_{ms}$ 」を用いて、下記式 (10) に基づいて MAC 演算を行い、セッション鍵データ Se_k を生成する。

当該セッション鍵データ Se_k は、正当な相手同士であれば、携帯用プレーヤ 4 で生成したセッション鍵データ Se_k と同じになる。

【0069】

【数10】

$$\text{セッション鍵データ } Se_k = \text{MAC} (IK_j, S_d \parallel S_{ms}) \quad \dots (10)$$

【0070】

〔携帯用記憶装置 3 へのオーディオデータの書き込み処理 (図 12 に示すステップ S6)〕

図 16 は、携帯用プレーヤ 4 から携帯用記憶装置 3 へのオーディオデータの書き込み処理を説明するための図である。

なお、当該書き込み処理を開始するときには、前述した図 15 に示すセッション鍵データ Se_k の生成処理は終了しており、携帯用記憶装置 3 および携帯用プレーヤ 4 は同じセッション鍵データ Se_k を有している。

【0071】

ステップ S40：携帯用プレーヤ 4 は、乱数発生ユニット 60 にトラックデータファイル毎に乱数を発生させ、当該乱数に応じたトラック鍵データ TRK を生成する。

【0072】

ステップ S41：携帯用プレーヤ 4 は、暗号化／復号ユニット 64 において、ステップ S40 で生成したトラック鍵データ TRK を、セッション鍵データ Se_k

k を用いて暗号化する。

【 0 0 7 3 】

ステップ 4 2 : 携帯用プレーヤ 4 は、ステップ S 4 1 で暗号化したトラック鍵データ TRK を携帯用記憶装置 3 に出力する。

【 0 0 7 4 】

ステップ S 4 3 : 携帯用記憶装置 3 は、ステップ S 4 2 で入力した暗号化されたトラック鍵データ TRK を、暗号化／復号ユニット 5 4 において復号する。

【 0 0 7 5 】

ステップ S 4 4 : 携帯用記憶装置 3 は、暗号化／復号ユニット 5 4 において、ステップ S 4 3 で復号したトラック鍵データ TRK を、記憶ユニット 5 1 から読み出した記憶用鍵データ SK_m を用いて暗号化する。

携帯用記憶装置 3 は、当該暗号化したトラック鍵データ TRK を、フラッシュメモリ 3 4 に記憶されているトラック管理ファイル 1 0 0 内の当該トラックデータに対応する TRK INF (n) 内に設定する。

【 0 0 7 6 】

ステップ S 4 5 : 携帯用プレーヤ 4 は、乱数発生ユニット 6 0 にパーツ毎に乱数を発生させ、当該乱数に応じたパーツ鍵データ PK を生成する。また、携帯用プレーヤ 4 は、当該生成したパーツ鍵データ PK を、携帯用記憶装置 3 のフラッシュメモリ 3 4 に記憶されている図 5 および図 6 に示すトラック管理ファイル 1 0 0 のうち対応するトラックデータファイルの管理データ PRT INF (N) 内に設定する。

【 0 0 7 7 】

ステップ S 4 6 : 携帯用プレーヤ 4 は、例えば、パーツ毎に、鍵生成／演算ユニット 6 2 において、下記式 (1 1) に示すように、ステップ S 4 5 で生成したパーツ鍵データ PK とトラック鍵データ TRK との排他的論理和を演算し、当該演算結果をテンポラリ鍵データ TMK とする。

なお、テンポラリ鍵データ TMK の生成は、排他的論理和を用いるものには限定されず、例えば、パーツ鍵データ PK とトラック鍵データ TRK とを加算する加算演算やその他の関数演算を用いるようにしてもよい。

【0078】

【数 11】

$$TMK = PK \quad XOR \quad TRK \quad \dots (11)$$

【0079】

ステップ S47: 携帯用プレーヤ 4 は、乱数発生ユニット 60 にクラスタ毎に乱数を発生させ、当該乱数に応じたクラスタシードデータ CS を生成する。また、携帯用プレーヤ 4 は、当該生成したクラスタシードデータ CS を、携帯用記憶装置 3 のフラッシュメモリ 34 に記憶されている当該クラスタ内の図 8 に示す対応する位置に設定する。

【0080】

ステップ S48: 携帯用プレーヤ 4 は、例えば、鍵生成/鍵演算ユニット 62 において、下記式 (12) に示すように、ステップ S46 で生成したテンポラリ鍵データ TMK と、ステップ S47 で生成したクラスタシードデータ CS とを用いて MAC 演算を行い、クラスタ毎にクラスタ鍵データ CK を生成する。

【0081】

【数 12】

$$CK = MAC (TMK, CS) \quad \dots (12)$$

【0082】

なお、MAC 演算の他に、例えば、SHA-1 (Secure Hash Algorithm)、RIPEMD-160 などの一方向性ハッシュ関数 (one-way hash function) の入力に秘密鍵を用いた演算を行ってクラスタ鍵データ CK を生成してもよい。

ここで、一方向性関数 f とは、 x より $y = f(x)$ を計算することは容易であるが、逆に y より x を求めることが難しい関数をいう。

なお、一方向性ハッシュ関数については、例えば、"Handbook of Applied Cryptography, CRC Press" などに詳しく記述されている。

【0083】

ステップ S49: 携帯用プレーヤ 4 は、コンピュータ 2 あるいは携帯用プレーヤ 4 から入力したオーディオデータを、圧縮/伸長モジュール 45 において、ATRAC3 方式で圧縮する。そして、暗号化/復号ユニット 64 において、ステ

ップ S 4 8 で生成したクラスタ鍵データ C K を用いて、前記圧縮したオーディオデータを C B C モードで暗号化する。

【0084】

ステップ S 5 0 : 携帯用プレーヤ 4 は、ステップ S 4 9 で暗号化したオーディオデータを、通信インタフェース 3 2 , 4 2 を介して、携帯用記憶装置 3 に出力する。

【0085】

ステップ S 5 1 : 携帯用記憶装置 3 は、ステップ S 5 0 で入力した暗号化されたオーディオデータを、フラッシュメモリ 3 4 にそのまま書き込む。

以上により、携帯用プレーヤ 4 から携帯用プレーヤ 4 へのオーディオデータの書き込み処理が終了する。

【0086】

携帯用記憶装置 3 からの読み出し動作

図 1 7 は、携帯用記憶装置 3 から携帯用プレーヤ 4 への読み出し動作を説明するためのフローチャートである。

ステップ S 6 1 : 携帯用プレーヤ 4 から携帯用記憶装置 3 に、読み出しを要求するトラックデータ（曲）を特定した読み出し要求信号が出力される。

ステップ S 2 : 図 1 3 を用いた前述したように、携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証処理を行う際に用いる認証鍵データ $I K_j$ の選択処理が行われる。

ステップ S 3 : 図 1 4 を用いて前述したように、携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証処理が行われる。

ステップ S 4 : ステップ S 3 の相互認証処理によって携帯用記憶装置 3 および携帯用プレーヤ 4 の双方が相手を正当であると認めた場合には、ステップ S 5 の処理が行われ、そうでない場合には処理が終了する。

ステップ S 5 : 携帯用記憶装置 3 および携帯用プレーヤ 4 において、セッション鍵データ S e k が生成される。

ステップ S 6 3 : 暗号化されたオーディオデータを、通信インタフェース 3 2 , 4 2 を介して、携帯用記憶装置 3 から携帯用プレーヤ 4 に読み出す。当該処理

については後述する。

すなわち、オーディオシステム 1 では、携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、後述するように、携帯用プレーヤ 4 において、携帯用記憶装置 3 から携帯用プレーヤ 4 に出力された暗号化されたトラック鍵データ TRK を適切なセッション鍵データ $Se k$ で解読できる。

そのため、著作権侵害を招くようなオーディオデータの不正な利用が容易に行われることを回避できる。

【0087】

〔携帯用記憶装置 3 からのオーディオデータの読み出し処理（図 17 に示すステップ S 63）〕

図 18 は、携帯用記憶装置 3 から携帯用プレーヤ 4 へのオーディオデータの読み出し処理を説明するための図である。

なお、当該読み出し処理は、前述した図 12 に示す書き込み処理の後に行われるため、図 4 に示すトラックデータファイル $101_0 \sim 101_3$ には、図 6 に示すように、各トラックデータファイルの管理データ $TRINF(n)$ にトラック鍵データ TRK が設定され、パーツ毎にパーツ鍵データ PK が設定され、図 8 に示すように各クラスタ CL 内にはクラスタシードデータ CS が設定されている。

また、ステップ S 5 の処理が終了しているため、携帯用記憶装置 3 および携帯用プレーヤ 4 は、正当な相手同士であれば、同じセッション鍵データ $Se k$ を有している。

【0088】

ステップ S 71：携帯用記憶装置 3 の暗号化／復号ユニット 54 は、図 4 に示すようにフラッシュメモリ 34 に記憶されている図 5 に示すトラック管理ファイル 100 内の $TRKINF(n)$ のうち、読み出し要求信号で特定されるトラックデータファイルに対応する $TRKINF(n)$ 内のトラック鍵データ TRK を、記憶ユニット 51 に記憶されている記憶用鍵データ SK_m を用いて復号する。

【0089】

ステップ S 72：携帯用記憶装置 3 の暗号化／復号ユニット 54 は、ステップ

S71で復号したトラック鍵データTRKを、図17に示すステップS5で得られたセッション鍵データSekを用いて暗号化する。

【0090】

ステップS73：携帯用記憶装置3は、ステップS72で暗号化したトラック鍵データTRKを携帯用プレーヤ4に出力する。

【0091】

ステップS74：携帯用プレーヤ4の暗号化／復号ユニット64は、ステップS73で携帯用記憶装置3から入力したトラック鍵データTRKを、セッション鍵データSekを用いて復号する。

【0092】

ステップS75：携帯用プレーヤ4の鍵生成／演算ユニット62は、ステップS74で復号されたトラック鍵データTRKと、携帯用記憶装置3のフラッシュメモリ34に記憶されているトラック管理ファイル100内の当該トラックデータファイルに対応するPRTINF(n)に含まれるパーツ鍵データPKとの排他的論理和を演算し、当該演算結果をテンポラリ鍵データTMKとする。

【0093】

【数13】

$$TMK = PK \text{ XOR } TRK \quad \dots (13)$$

【0094】

ステップS76：携帯用プレーヤ4の鍵生成／鍵演算ユニット62において、ステップS75で生成したテンポラリ鍵データTMKと、携帯用記憶装置3のフラッシュメモリ34に記憶されている当該トラックデータファイルに対応するトラックデータファイル101₀～101₃のクラスタ内の図8に示すクラスタシードデータCSとを用いて、下記式(14)に示すMAC演算を行い、当該演算結果をクラスタ鍵データCKとする。

クラスタ鍵データCKは、クラスタ毎に求められる。

【0095】

【数14】

$$CK = MAC(TMK, CS) \quad \dots (14)$$

【0096】

ステップS77：携帯用記憶装置3は、フラッシュメモリ34に記憶されている図4に示すトラックデータファイル101₀～10₃のうち読み出し要求信号で特定されるトラックデータファイルに対応するトラックデータファイルを特定し、当該特定したトラックデータファイルを構成するクラスタ内のオーディオデータを、図8に示すサウンドユニットSUを単位として読み出して携帯用プレーヤ4に出力する。

【0097】

ステップS78：携帯用プレーヤ4は、暗号化／復号ユニット64において、ステップS76で生成したクラスタ鍵データCKを用いて、ステップS77で入力したオーディオデータを復号する。

このとき、オーディオデータの復号は、各クラスタ毎に、それぞれ個別に求められたクラスタ鍵データCKを用いて行われる。また、復号は、暗号化の単位である8バイトのブロックを単位として行われる。

【0098】

ステップS79：携帯用プレーヤ4は、圧縮／伸長モジュール45において、ステップS78で復号したオーディオデータをATRAC3方式で伸長し、当該伸長したオーディオデータを、D/A変換器47でデジタル形式に変換した後に、スピーカ46に出力する。

このとき、圧縮／伸長モジュール45は、ステップS78で復号したオーディオデータを、サウンドユニットSUを単位として伸長する。

【0099】

以上により、携帯用記憶装置3から携帯用プレーヤ44へのオーディオデータの読み出しおよび再生が終了する。

【0100】

〔トラックデータファイルの分割編集処理〕

前述したように、携帯用プレーヤ4の編集モジュール44は、1個のトラックデータファイルを分割して2個のトラックデータファイルを生成する分割編集処理と、2個のトラックデータファイルを結合して1個のトラックデータファイル

を生成する結合編集処理とを行う。

まず、分割編集処理について説明する。

図19は、携帯用プレーヤ4の編集モジュール44によるトラックデータファイルの分割編集処理を説明するための図である。

編集モジュール44は、例えば、図19(A)に示す1個のトラックデータファイル(1)を、図19(B)に示すトラックデータファイル(1)と、図19(C)に示すトラックデータファイル(2)とに分割する。

このとき、分割の区切りとなる最小単位はサウンドユニットSUであり、当該例では、図19(B)に示すように、トラックデータファイル(1)のクラスタCL(2)のサウンドユニットSU(3)とSU(4)との間で分割されている。

【0101】

当該分割により、分割後のトラックデータファイル(1)のクラスタCL(2)は図20(A)に示すようになり、新たに生成されたトラックデータファイル(2)のクラスタCL(0)は図20(B)に示すようになる。

このとき、図20(B)に示すように、トラックデータファイル(2)のクラスタCL(0)のサウンドユニットSU(0)は分割前のトラックデータファイル(1)のクラスタ(2)のサウンドユニットSU(4)となり、トラックデータファイル(2)のクラスタCL(0)のサウンドユニットSU(1)は分割前のトラックデータファイル(1)のクラスタ(2)のサウンドユニットSU(5)となる。

また、図20(B)に示すトラックデータファイル(2)のクラスタCL(0)のブロック暗号化初期値IVには、図19(A)，(B)に示すトラックデータファイル(1)のクラスタCL(2)内のサウンドユニットSU(3)の最後の8バイトが設定される。

本実施形態では、前述したように各クラスタ内において、最初のサウンドユニットSU(0)の直前にブロック暗号化初期値IVを配置したことで、分割の際に、分割位置の直前の8バイトをそのままブロック暗号化初期値IVとして用いれば良く、新たなトラックデータファイルを作成する際の処理を簡単にできる。

また、再生時に、サウンドユニットSU(0)と共に、その直前のブロック暗号化初期値IVを読み出せばよいため、再生処理も簡単になる。

【0102】

本実施形態では、分割前のトラックデータファイル(1)のトラック鍵データ、パーツ鍵データおよびクラスタ鍵データは、それぞれTRK__1、PK__1およびCK__1である。

また、分割後のトラックデータファイル(1)のトラック鍵データ、パーツ鍵データおよびクラスタ鍵データは、それぞれTRK__1'、PK__1'およびCK__1である。

また、トラックデータファイル(2)のトラック鍵データ、パーツ鍵データおよびクラスタ鍵データは、それぞれTRK__2、PK__2およびCK__1である。

【0103】

図21は、携帯用プレーヤ4の編集モジュール44において、新たなトラックデータファイル(2)のトラック鍵データおよびパーツ鍵データを生成する方法を説明するための図である。

分割により生成された新たなトラックデータファイル(2)は、トラックデータファイル(1)とは別に新たなトラック鍵データTRK__2を有する。本実施形態では、パーツ鍵データPK__2を以下に示すように算出することで、クラスタ鍵データCK__1を分割前と同じにする。

【0104】

ステップS90：編集モジュール44は、トラックデータファイルの分割指示を入力したか否かを判断し、入力したと判断した場合にはステップS91の処理を実行し、入力していないと判断した場合にはステップS90の処理を繰り返す。

【0105】

ステップS91：編集モジュール44は、乱数発生ユニット60に乱数を発生させ、当該乱数に応じたトラック鍵データTRK__2を新たに生成する。

【0106】

ステップS92：編集モジュール44は、トラックデータファイル（2）のパーツ鍵データPK__2を下記式（15）に基づいて生成する。

【0107】

【数15】

$$PK_2 = TRK_1 \text{ XOR } PK_1 \text{ XOR } TRK_2$$

…（15）

【0108】

これにより、トラックデータファイル（2）について、前記式（11）に基づいてされるテンポラリ鍵データは、トラックデータファイル（1）のテンポラリ鍵データと同じになり、前記式（12）に基づいて生成されるクラスタ鍵データも分割前のクラスタ鍵データCK__1と同じにできる。

そのため、トラックデータファイル（2）内のサウンドユニットSUを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

【0109】

ステップS93：携帯用記憶装置3の暗号化／復号ユニット54において、ステップS91で生成したトラック鍵データTRK__2を、記憶ユニット51に記憶されている記憶用鍵データSK_mを用いて暗号化し、当該暗号化したトラック鍵データTRK__2を、フラッシュメモリ34に記憶されているトラック管理ファイル100内の当該トラックデータファイルに対応する図6に示すTRKINFに書き込む。

【0110】

ステップS94：編集モジュール44は、ステップS92で生成したパーツ鍵データPK__2を、フラッシュメモリ34に記憶されているトラック管理ファイル100内の当該トラックデータファイルに対応する図6に示すPRTINFにそのまま書き込む。

【0111】

このように、オーディオシステム1では、分割して新たに生成したトラックデータファイル（2）のトラック鍵データとして、新たなトラック鍵データTRK

__2を用いた場合でも、上記式(15)に基づいてパーツ鍵データPK__2を生成することで、テンポラリ鍵データを分割前のテンポラリ鍵データと同じにできる。その結果、クラスタ鍵データも分割前のクラスタ鍵データCK__1と同じにでき、トラックデータファイル(2)内のサウンドユニットSUを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

また、同様に、分割後のトラックデータファイル(1)のパーツ鍵データPK__1'も、クラスタ鍵データCK__1を変えないように、トラック鍵データTRK__1'に応じた決定される。その結果、分割後のトラックデータファイル(1)内のサウンドユニットSUを新たなクラスタ鍵データを用いて再度暗号化する必要もない。

そのため、トラックデータファイルの分割編集に伴い演算量が大幅に増加することを回避できる。

【0112】

次に、トラックデータファイルの結合編集処理について説明する。

図22は、携帯用プレーヤ4の編集モジュール44によるトラックデータファイルの結合編集処理を説明するための図である。

図22に示すように、編集モジュール44は、例えば、図22(A)に示すトラックデータファイル(1)と、図22(B)に示すトラックデータファイル(2)とを結合して、図22(C)に示すトラックデータファイル(3)を生成する。

【0113】

当該結合により、結合前のトラックデータファイル(1)からなるパーツ(1)と、結合前のトラックデータファイル(2)からなるパーツ(2)とを含む新たなトラックデータファイル(3)が生成される。

また、トラックデータファイル(3)のトラック鍵データとして新たなトラック鍵データTRK__3が生成され、パーツ(1)のパーツ鍵データPK__3__1およびパーツ(2)のパーツ鍵データPK__3__2が後述するようにして新たに生成される。

また、トラック管理ファイル100に、当該トラックデータファイル(3)に

対応する図6に示すTRKINFおよびPRTINFが追加され、当該TRKINFおよびPRTINFに、新たに生成された鍵データが後述するように設定される。

また、パーツ(1)の図6に示すPRTSIZEが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル(1)のクラスタCL(0)およびCL(4)がそれぞれ設定される。また、パーツ(2)のPRTSIZEが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル(2)のクラスタCL(0)およびCL(5)がそれぞれ設定される。

【0114】

図23は、携帯用プレーヤ4の編集モジュール44において、新たに生成したトラックデータファイル(3)のパーツ(1)および(2)のパーツ鍵データを生成する処理を説明するための図である。

なお、本実施形態では、結合の対象となるトラックデータファイル(1)がトラック鍵データTRK__1、パーツ鍵データPK__1およびクラスタ鍵データCK__1を用いており、トラックデータファイル(2)がトラック鍵データTRK__2、パーツ鍵データPK__2およびクラスタ鍵データCK__2を用いてる場合を例示して説明する。

【0115】

ここで、トラックデータファイル(3)は新たなトラック鍵データTRK__3を得るが、パーツ(1)および(2)のパーツ鍵データを以下に示すように算出することで、各クラスタのクラスタ鍵データCK__1およびCK__2を結合前と同じにできる。

【0116】

ステップS100：編集モジュール44は、トラックデータファイルの結合指示を入力したか否かを判断し、入力したと判断した場合にはステップS101の処理を実行し、入力していないと判断した場合にはステップS100の処理を繰り返す。

【0117】

ステップS101：編集モジュール44は、乱数発生ユニット60に乱数を発

生させ、当該乱数に応じたトラック鍵データ TRK__3 を新たに生成する。

【0118】

ステップ S102：編集モジュール 44 は、トラックデータファイル（3）のパーツ（1）のパーツ鍵データ PK__3__1 を下記式（16）に基づいて生成する。

【0119】

【数16】

$$PK_3_1 = TRK_1 \text{ XOR } PK_1 \text{ XOR } TRK_3 \\ \dots (16)$$

【0120】

これにより、前記式（11）に基づいて生成されるパーツ（1）のテンポラリ鍵データを結合前のトラックデータファイル（1）のテンポラリ鍵データと同じにでき、その結果、前記式（12）に基づいて生成されるパーツ（1）のクラスタ鍵データも結合前のトラックデータファイル（1）のクラスタ鍵データ CK__1 と同じにできる。

そのため、パーツ（1）のサウンドユニット SU を新たなクラスタ鍵データを用いて再度暗号化する必要がない。

【0121】

ステップ S103：編集モジュール 44 は、トラックデータファイル（3）のパーツ（2）のパーツ鍵データ PK__3__2 を下記式（17）に基づいて生成する。

【0122】

【数17】

$$PK_3_2 = TRK_2 \text{ XOR } PK_2 \text{ XOR } TRK_3 \\ \dots (17)$$

【0123】

これにより、前記式（11）に基づいて生成されるパーツ（2）のテンポラリ鍵データを結合前のトラックデータファイル（2）のテンポラリ鍵データと同じにでき、その結果、前記式（12）に基づいて生成されるパーツ（2）のクラス

タ鍵データも結合前のトラックデータファイル（２）のクラスタ鍵データCK__2と同じにできる。

そのため、パーツ（２）のサウンドユニットSUを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

【0124】

ステップS104：携帯用記憶装置3の暗号化／復号ユニット54において、ステップS101で生成したトラック鍵データTRK__3を、記憶ユニット51に記憶されている記憶用鍵データSK_■を用いて暗号化し、当該暗号化したトラック鍵データTRK__3をフラッシュメモリ34内のトラックデータファイル（3）に対応する図6に示すTRKINFに書き込む。

【0125】

ステップS105：編集モジュール44は、ステップS102およびS103で生成したパーツ鍵データPK__3__1およびPK__3__2をフラッシュメモリ34内のトラックデータファイル（3）のそれぞれパーツ（１）およびパーツ（２）に対応する図6に示すPRTINFにそのまま書き込む。

【0126】

このように、オーディオシステム1では、結合して新たに生成したトラックデータファイル（3）のトラック鍵データとして、新たなトラック鍵データTRK__3を用いた場合でも、上記式（16）および（17）に基づいてパーツ鍵データPK__3__1およびPK__3__2を生成することで、各パーツのテンポラリ鍵データを結合前と同じにできる。その結果、各パーツのクラスタ鍵データも結合前のクラスタ鍵データCK__1およびCK__2とそれぞれ同じにでき、パーツ（１）および（２）内のサウンドユニットSUを新たなクラスタ鍵データを用いて再度暗号化する必要がない。そのため、トラックデータファイルの分割編集に伴い演算量が大幅に増加することを回避できる。

【0127】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ATRAC3方式の圧縮の単位であるサウンドユニットSUのバイト数（160バイト）が、CBCモードの暗号化の単位で

ある暗号化ブロックのバイト数（8バイト）の整数倍になる場合を例示したが、本発明は、例えば、整数倍にならない場合には、サウンドユニットSUにデータ長調整用のデータであるパディング(padding)を挿入して調整するようにしてもよい。

【0128】

また、上述した実施形態では、携帯用記憶装置3と携帯用プレーヤ4との間で相互認証処理を行う場合に、図14に示すように、先ず始めに携帯用記憶装置3で生成した乱数 R_{ms} を携帯用プレーヤ4に出力する場合を例示したが、先ず始めに携帯用プレーヤ4で生成した乱数を携帯用記憶装置3に出力するようにしてもよい。

【0129】

また、上述した実施形態では、図13に示すように、記憶ユニット51および61に32組の認証鍵データおよびマスター鍵データを記憶した場合を例示したが、これらの組の数は2以上であれば任意である。

【0130】

また、上述した実施形態では、図13に示すように、携帯用プレーヤ4において、マスター鍵データ $MK_0 \sim MK_{31}$ から認証鍵データ $IK_0 \sim IK_{31}$ を生成する場合を例示したが、携帯用プレーヤ4に、携帯用記憶装置3と同じように、認証鍵データ $IK_0 \sim IK_{31}$ を記憶し、乱数 R_j に応じた認証鍵データを選択するようにしてもよい。

【0131】

また、上述した実施形態では、図13に示すように、携帯用記憶装置3および携帯用プレーヤ4において、携帯用プレーヤ4で生成した乱数 R_j を用いて、認証鍵データ IK_j およびマスター鍵データ MK_j を選択する場合を例示したが、携帯用記憶装置3で生成した乱数を用いてもよいし、携帯用記憶装置3および携帯用プレーヤ4の双方で発生した乱数を用いてもよい。

【0132】

また、上述した実施形態では、図13に示すように、携帯用記憶装置3および携帯用プレーヤ4において乱数 R_j に基づいて認証鍵データ IK_j およびマスタ

一鍵データ MK_j を選択する場合を例示したが、本発明は、例えば、携帯用記憶装置3および携帯用プレーヤ4に外部から5ビットの鍵選択指示データを入力し、当該鍵選択指示データで指示される相互に対応する認証鍵データ IK_j およびマスター鍵データ MK_j を、携帯用記憶装置3および携帯用プレーヤ4で選択してもよい。

【0133】

また、上述した実施形態では、トラックデータとしてオーディオデータを含むデータを例示したが、本発明は、その他、動画像データ、静止画像データ、文書データおよびプログラムデータなどを含むトラックデータをフラッシュメモリ34に記憶する場合にも適用できる。

【0134】

【発明の効果】

以上説明したように、本発明のデータ処理装置、データ処理システムおよびその方法によれば、記憶手段に記憶された暗号化されたデータを、所定の処理ブロックを単位として効率的に処理できる。

【図面の簡単な説明】

【図1】

図1は、本発明の実施形態のオーディオシステムのシステム構成図である。

【図2】

図2は、図1に示す携帯用記憶装置および携帯用プレーヤの内部構成図である。

【図3】

図3は、図2に示す携帯用記憶装置内の記憶ユニットに記憶されているデータを説明するための図である。

【図4】

図4は、図2に示す携帯用記憶装置のフラッシュメモリに記憶されるデータを説明するための図である。

【図5】

図5は、図4に示すトラック管理ファイルのフォーマットを説明するための図

である。

【図 6】

図 6 は、図 5 に示す TRKINF および PRTINF の詳細なフォーマットを説明するための図である。

【図 7】

図 7 は、図 4 に示すトラックデータファイルの構成を説明するための図である。

【図 8】

図 8 は、図 7 に示すクラスタ CL の構成を説明するための図である。

【図 9】

図 9 は、図 2 に示す携帯用プレーヤの記憶ユニットに記憶されているデータを説明するための図である。

【図 10】

図 10 は、図 2 に示す携帯用プレーヤの暗号化／復号ユニットの CBC モードにおける暗号化処理を説明するための図である。

【図 11】

図 11 は、図 2 に示す携帯用プレーヤの暗号化／復号ユニットの CBC モードにおける復号処理を説明するための図である。

【図 12】

図 12 は、図 2 に示す携帯用プレーヤから携帯用記憶装置への書き込み動作を説明するためのフローチャートである。

【図 13】

図 13 は、図 2 に示す相互認証ユニットによる認証鍵データ IK_j の選択処理を説明するための図である。

【図 14】

図 14 は、図 2 に示す携帯用記憶装置と携帯用プレーヤとの間の相互認証処理を説明するための図である。

【図 15】

図 15 は、セッション鍵データ Se_k の生成処理を説明するための図である。

【図 16】

図 16 は、図 2 に示す携帯用プレーヤから携帯用記憶装置へのオーディオデータの書き込み処理を説明するための図である。

【図 17】

図 17 は、図 2 に示す携帯用記憶装置から携帯用プレーヤへの読み出し動作を説明するためのフローチャートである。

【図 18】

図 18 は、図 2 に示す携帯用記憶装置から携帯用プレーヤへのオーディオデータの読み出し処理を説明するための図である。

【図 19】

図 19 は、携帯用プレーヤの編集モジュールによるトラックデータファイルの分割編集処理を説明するための図である。

【図 20】

図 19 に示す分割編集処理を行った後のクラスタ内のデータを説明するための図である。

【図 21】

図 21 は、図 2 に示す携帯用プレーヤの編集モジュールにおいて、分割編集時に、新たなトラックデータファイルのトラック鍵データおよびパーツ鍵データを生成する方法を説明するための図である。

【図 22】

図 22 は、図 2 に示す携帯用プレーヤの編集モジュールによるトラックデータファイルの結合編集処理を説明するための図である。

【図 23】

図 23 は、図 2 に示す携帯用プレーヤ 4 の編集モジュールにおいて、新たに生成したトラックデータファイル (3) のパーツ (1) および (2) のパーツ鍵データを生成する処理を説明するための図である。

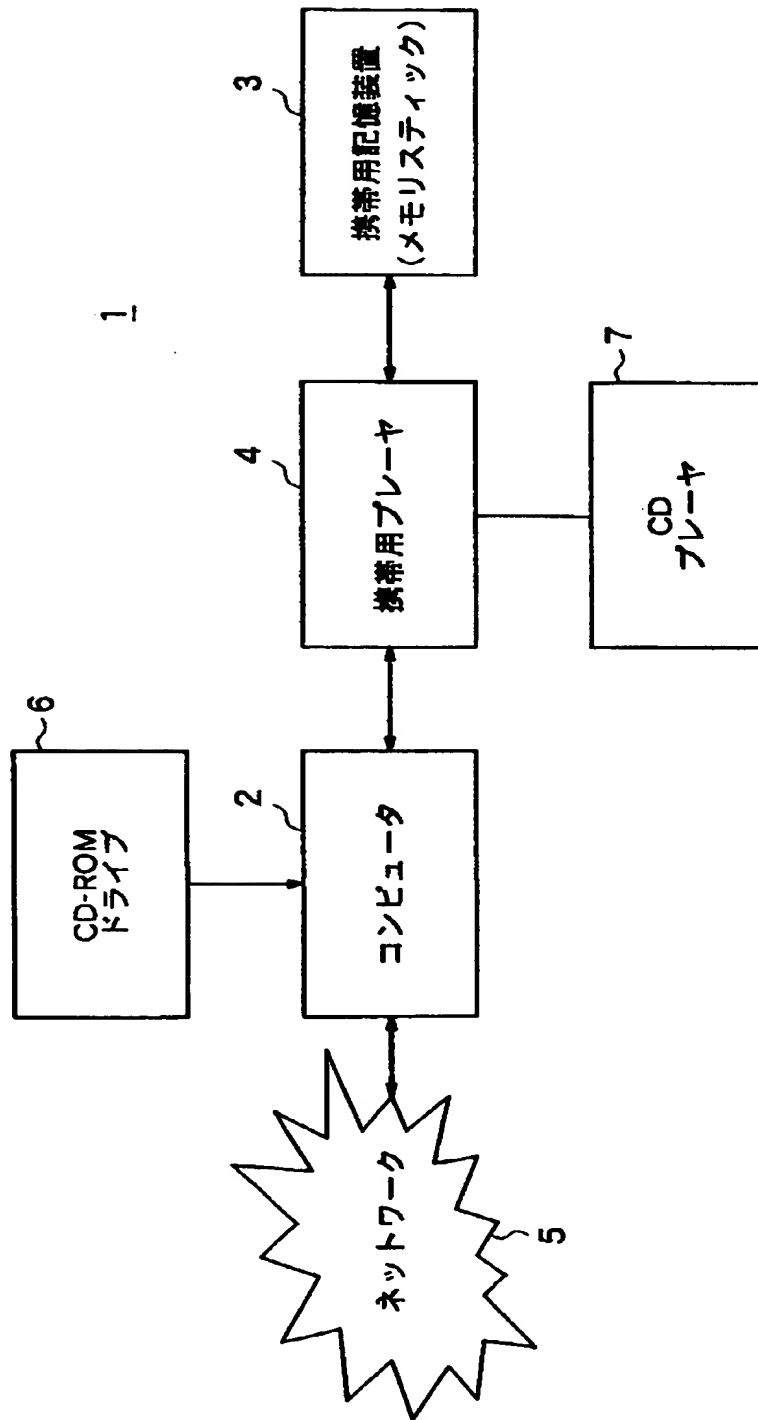
【符号の説明】

1…オーディオシステム、2…コンピュータ、3…携帯用記憶装置、4…携帯用プレーヤ、5…ネットワーク、33、43…制御モジュール、50、60…乱

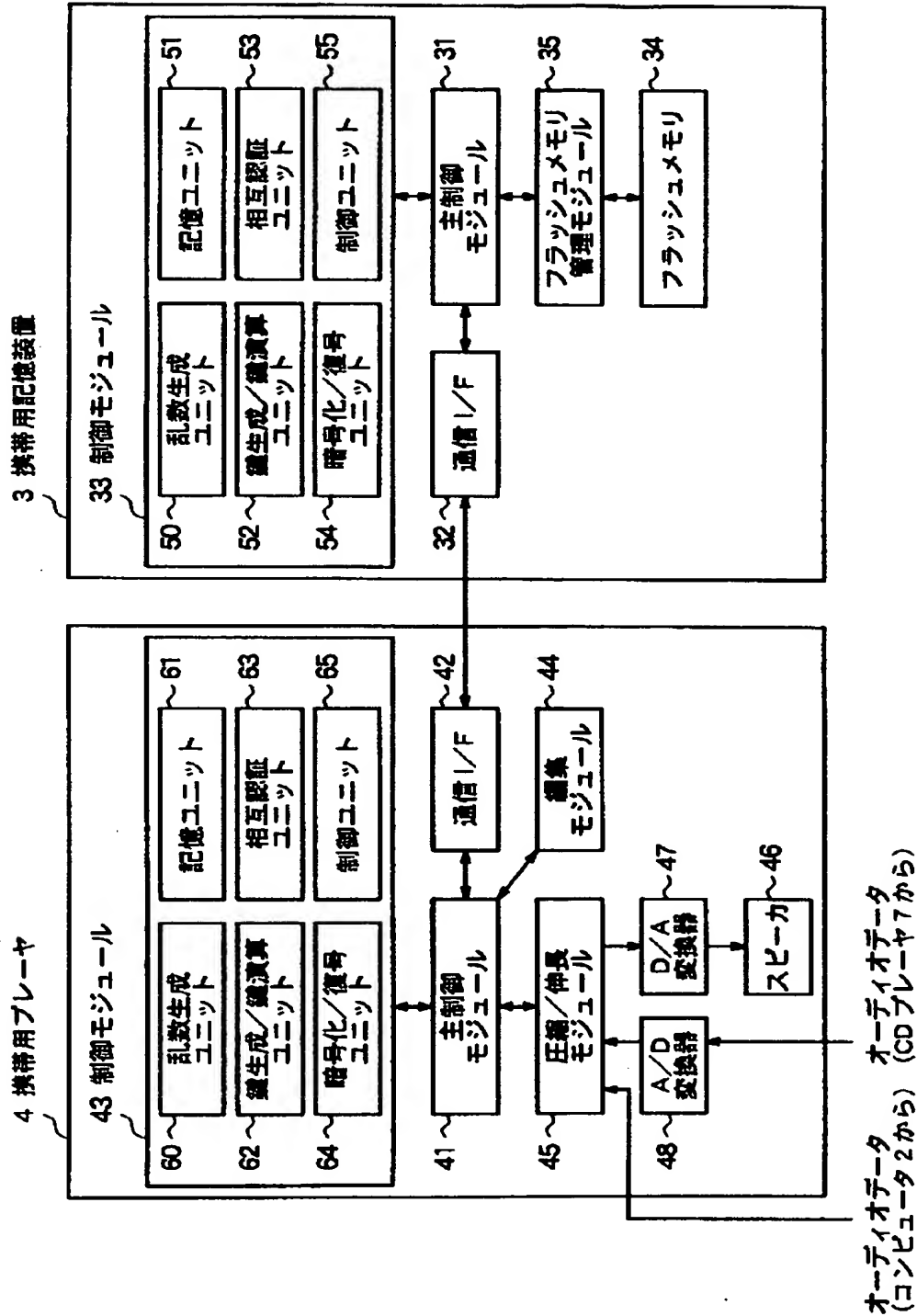
数発生ユニット、51, 61…記憶ユニット、52, 62…鍵生成／演算ユニット、53, 63…相互認証ユニット、54, 74…暗号化／復号ユニット、55, 65…制御ユニット、34…フラッシュメモリ、44…編集モジュール、45…圧縮／伸長モジュール、46…スピーカ

【書類名】 図面

【図 1】



【図 2】

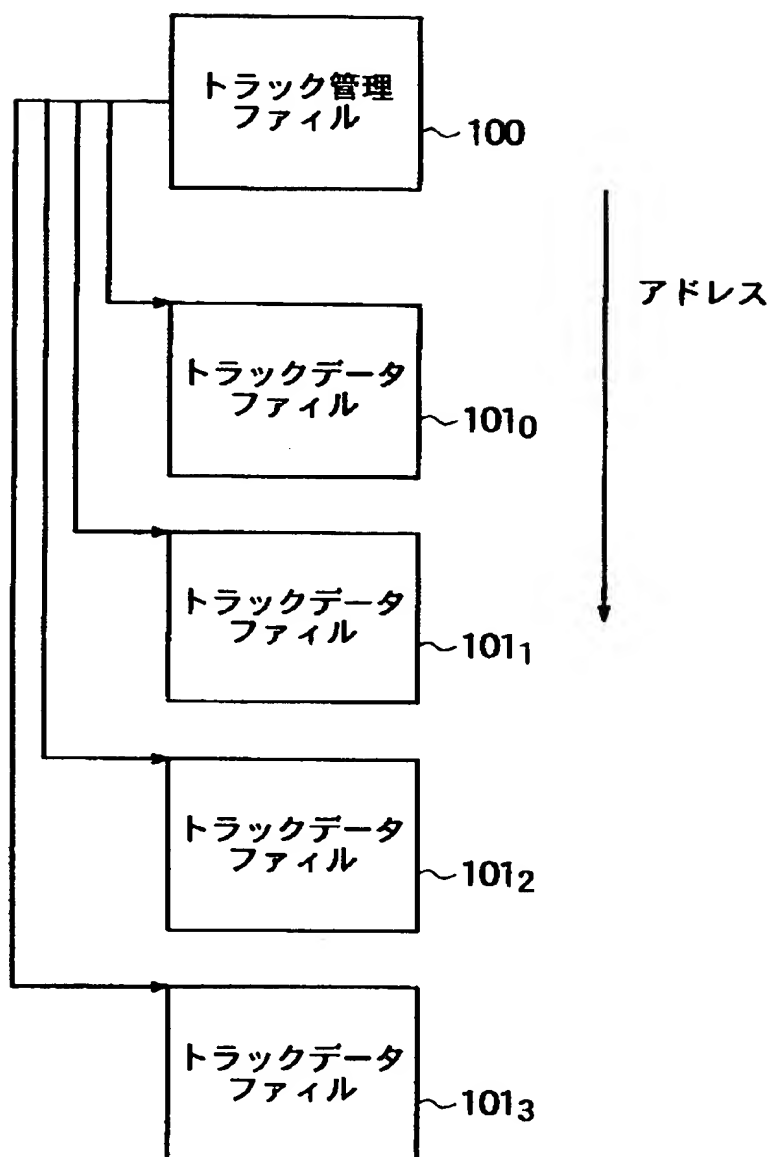


【図 3】

携帯用記憶装置 3 の記憶ユニット 51 に記憶されるデータ

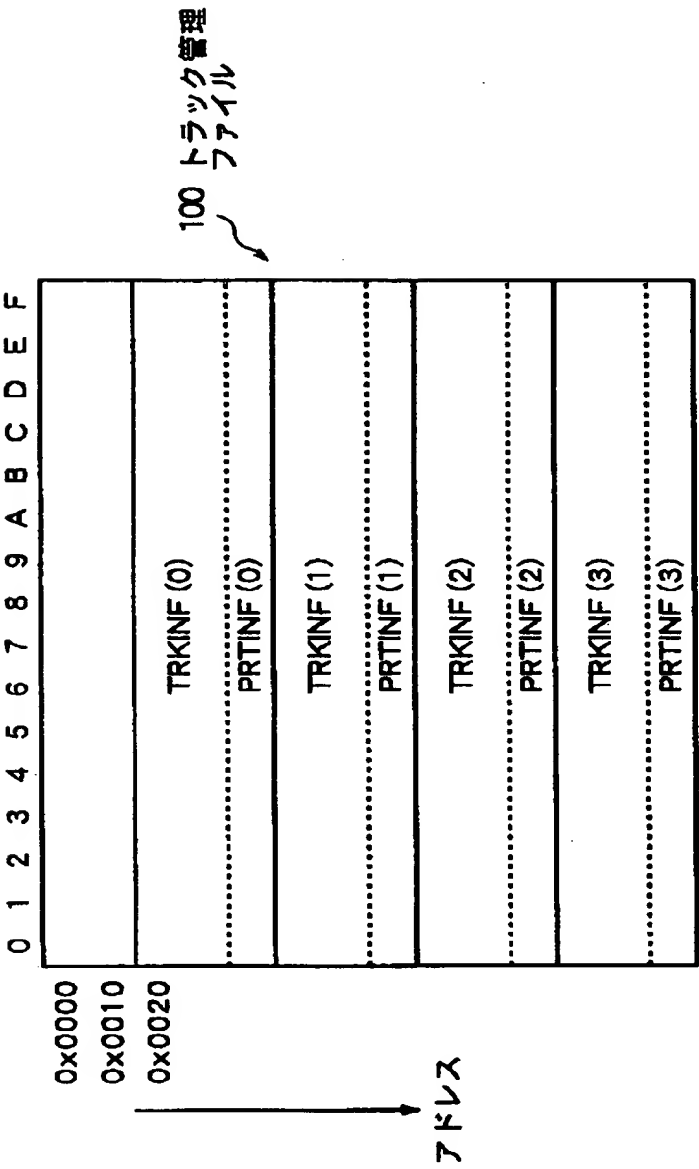
認証鍵データ IK_0
 IK_1
 IK_2
 IK_3
 \vdots
 IK_{30}
 IK_{31}
装置識別データ ID_m
記憶用鍵データ SK_m

【図 4】

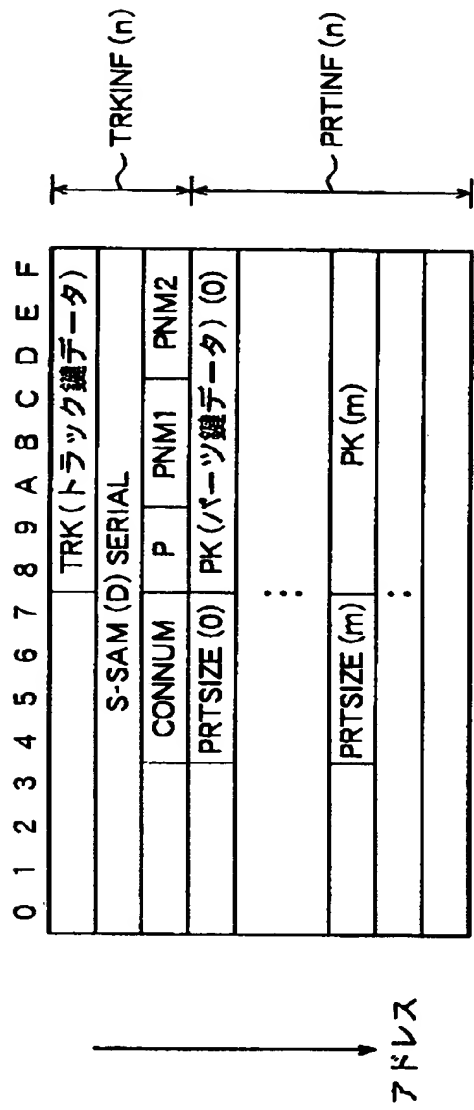


携帯用記憶装置 3 のフラッシュメモリ 34 の記憶データ

【図 5】

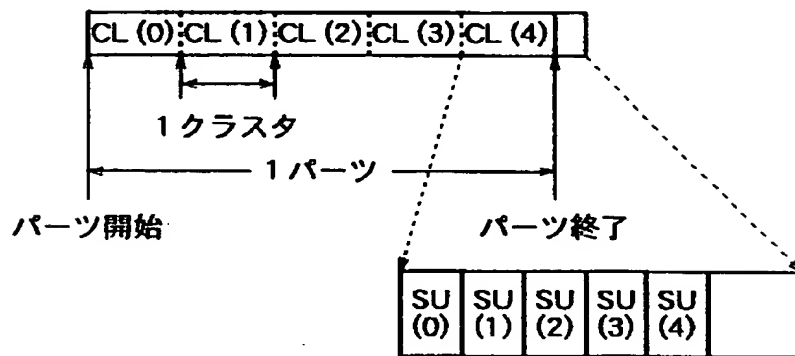


【図 6】

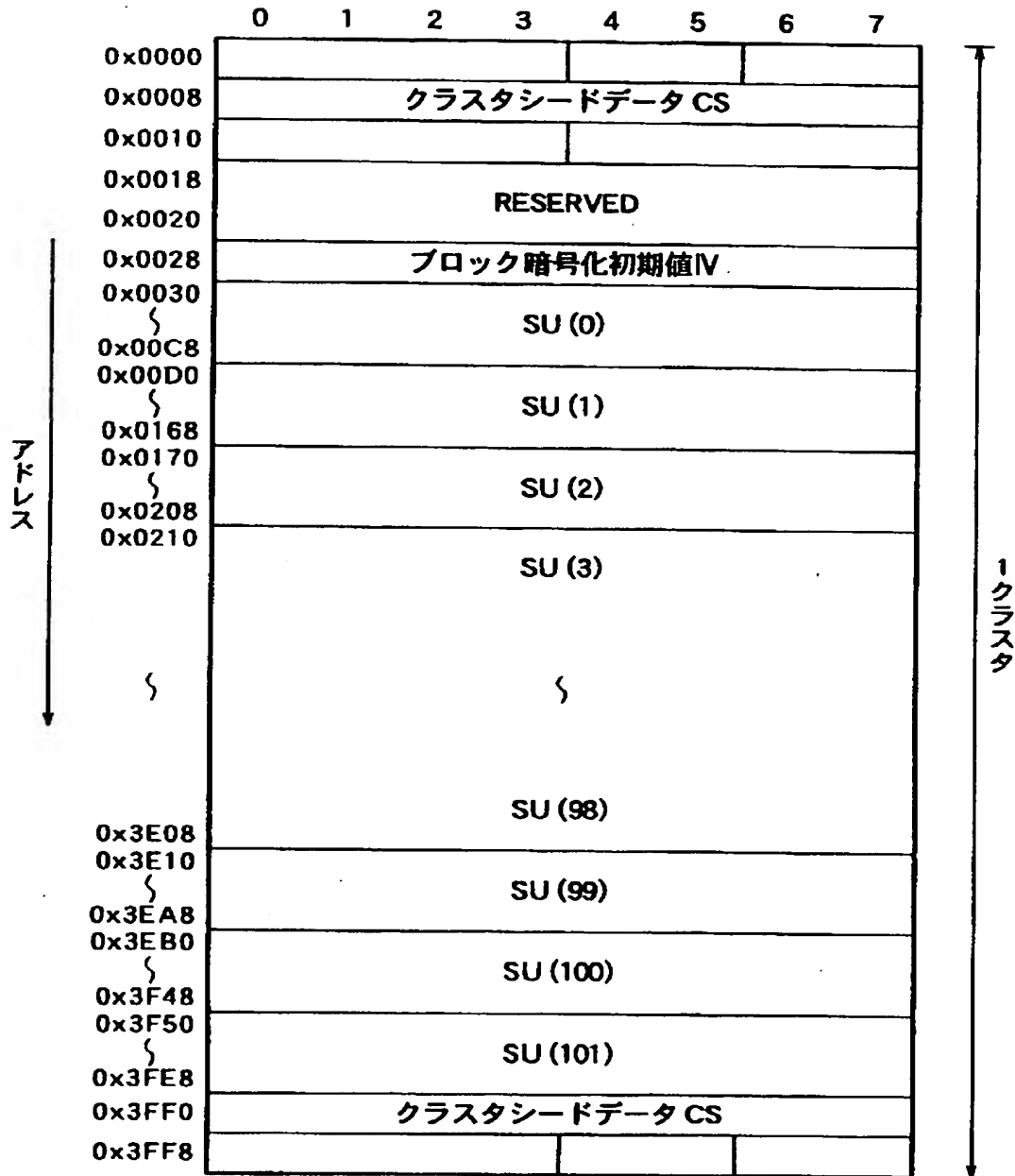


【図 7】

トラックデータファイル 101₀



【図 8】



【図 9】

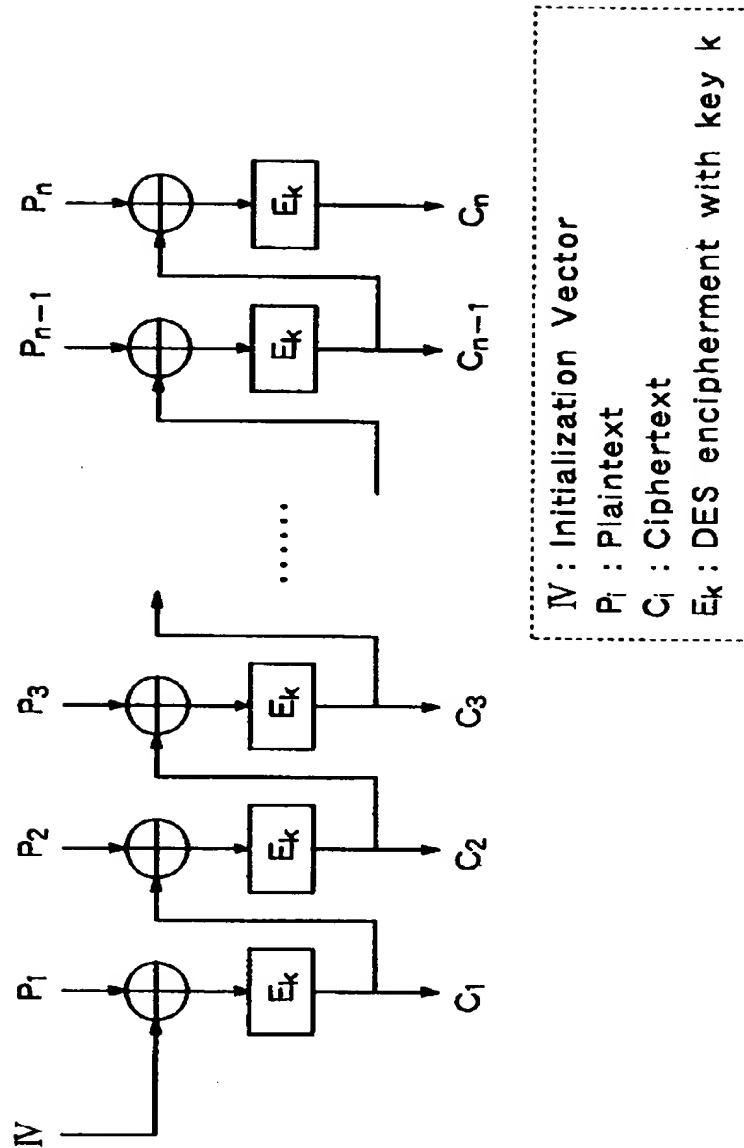
携帯用プレーヤ 4 の記憶モジュール 41 に記憶されるデータ

マスター鍵データ MK₀
MK₁
MK₂
MK₃
⋮
MK₃₀
MK₃₁
装置識別データ I D_d

【図 1 0】

DES CBC モード (暗号化)

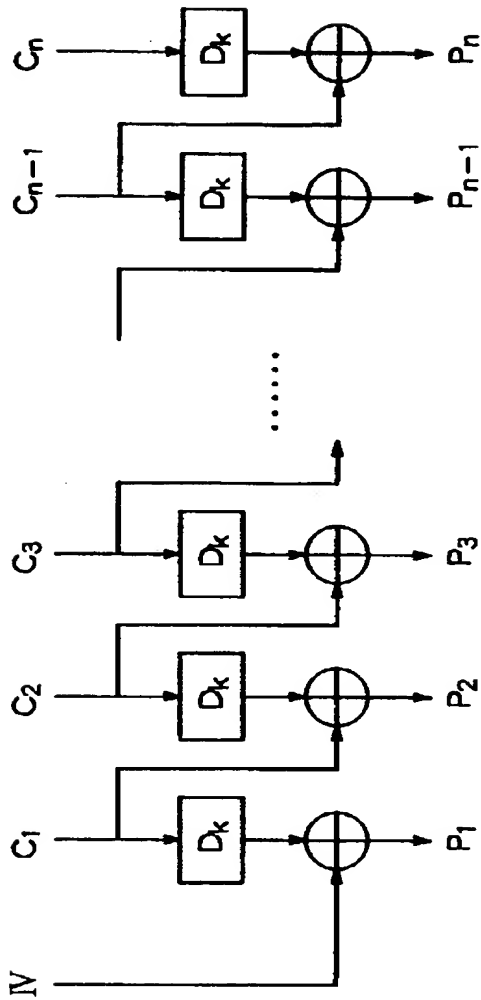
$$C_i = E_k (P_i \text{ XOR } C_{i-1})$$



【図 1 1】

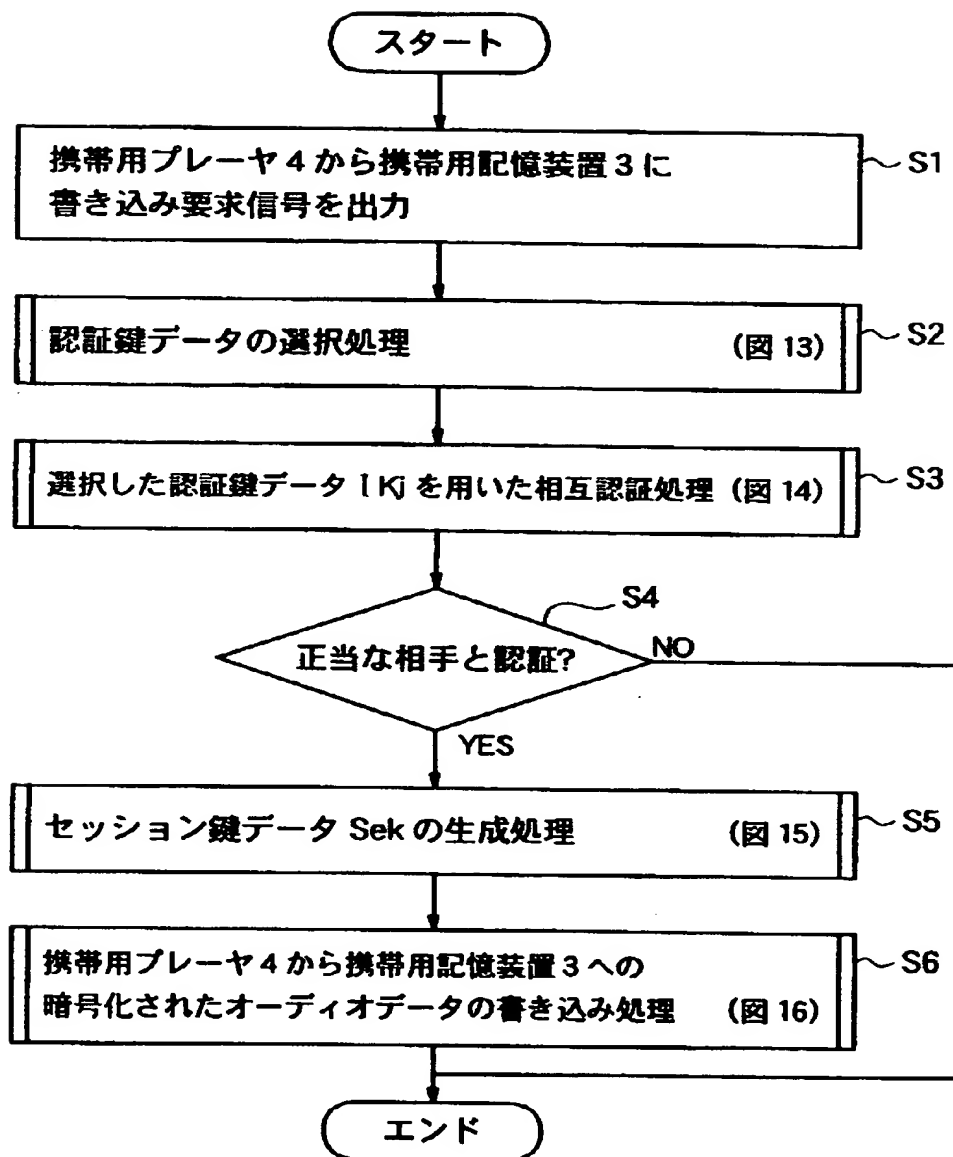
DES CBC モード (復号化)

$$P_i = C_{i-1} \text{ XOR } D_k(C_i)$$



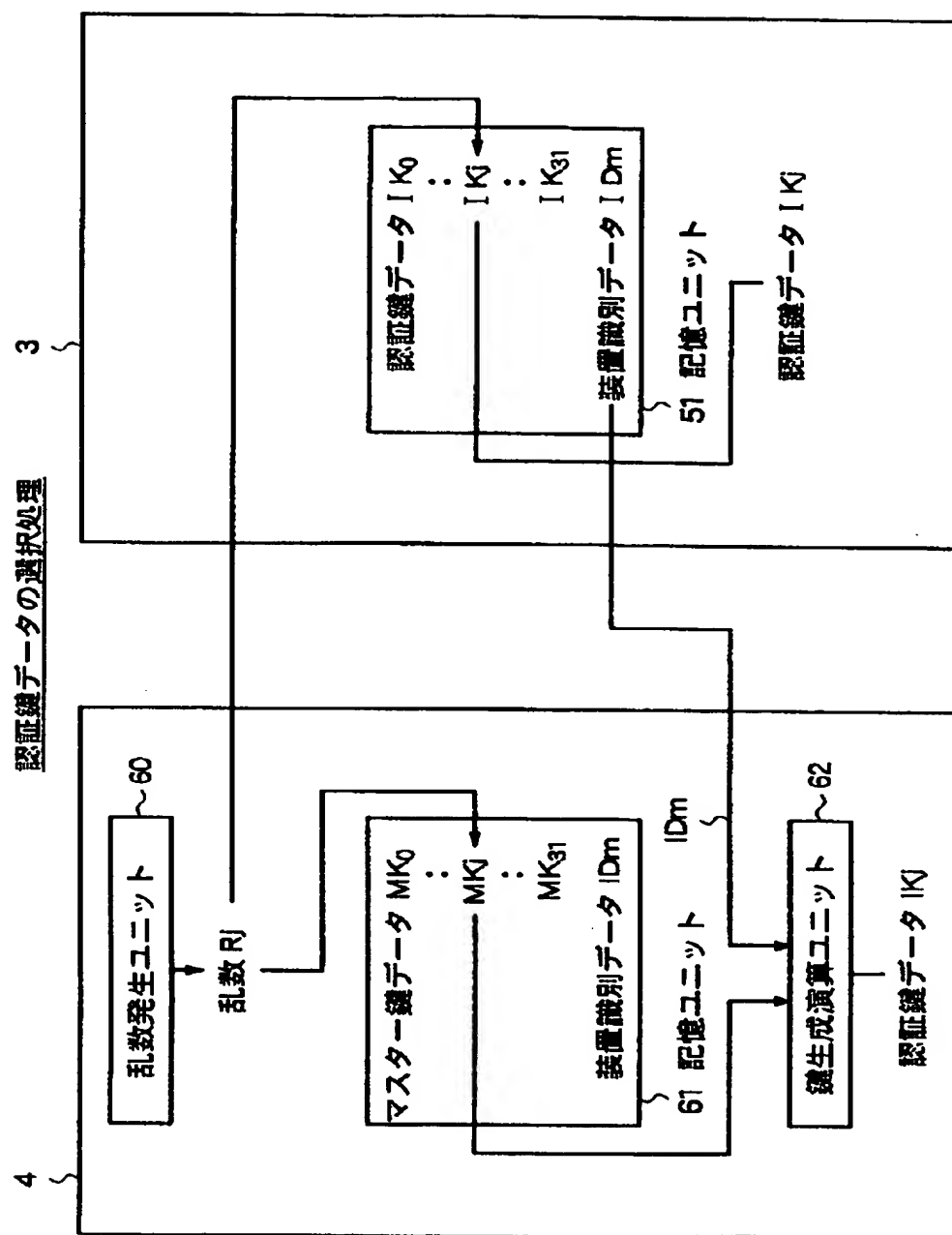
- IV : Initialization Vector
 P_i : Plaintext
 C_i : Ciphertext
 D_k : DES decipherment with key k

【図 12】

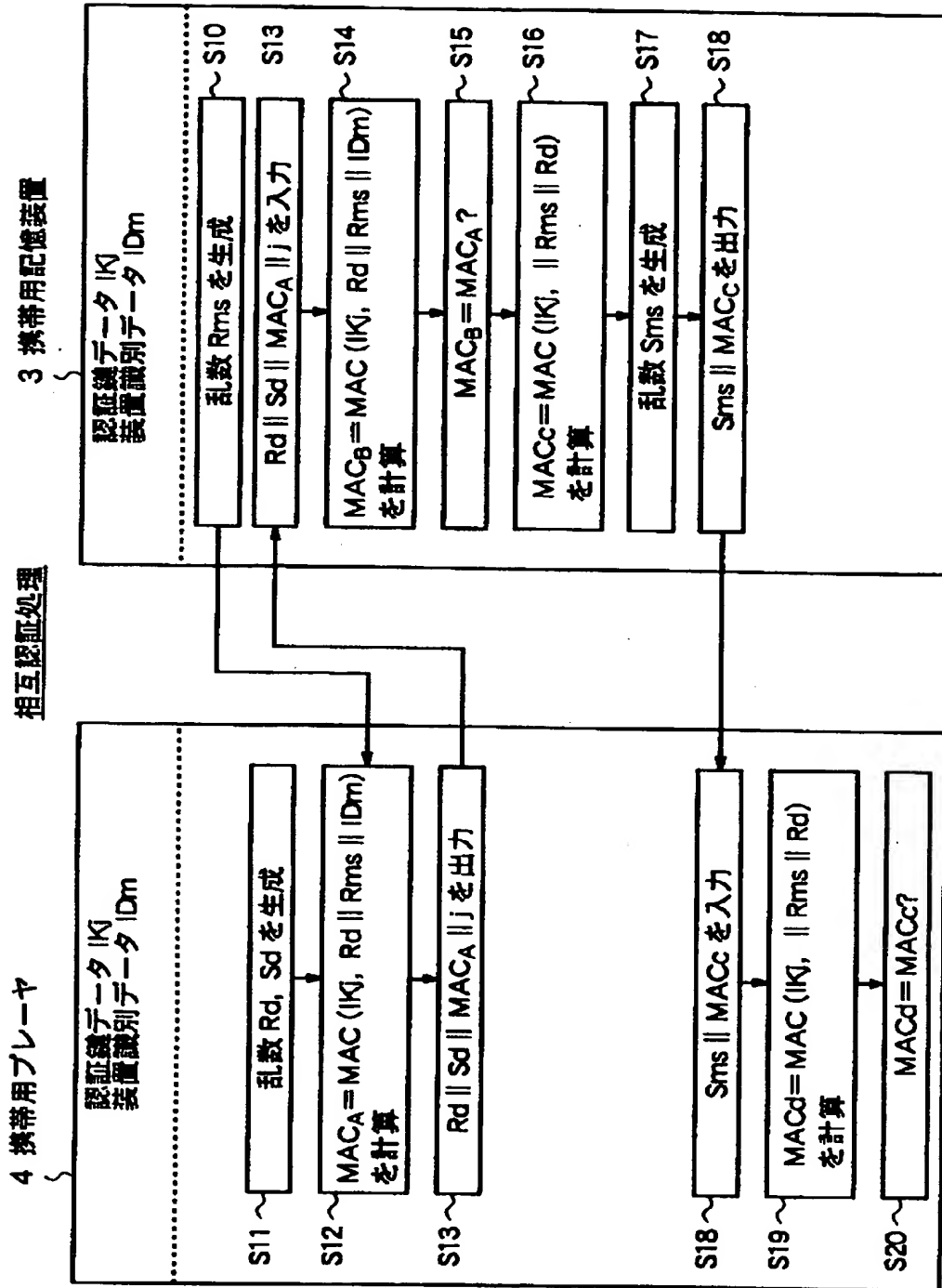


携帯用記憶装置 3 への書込処理

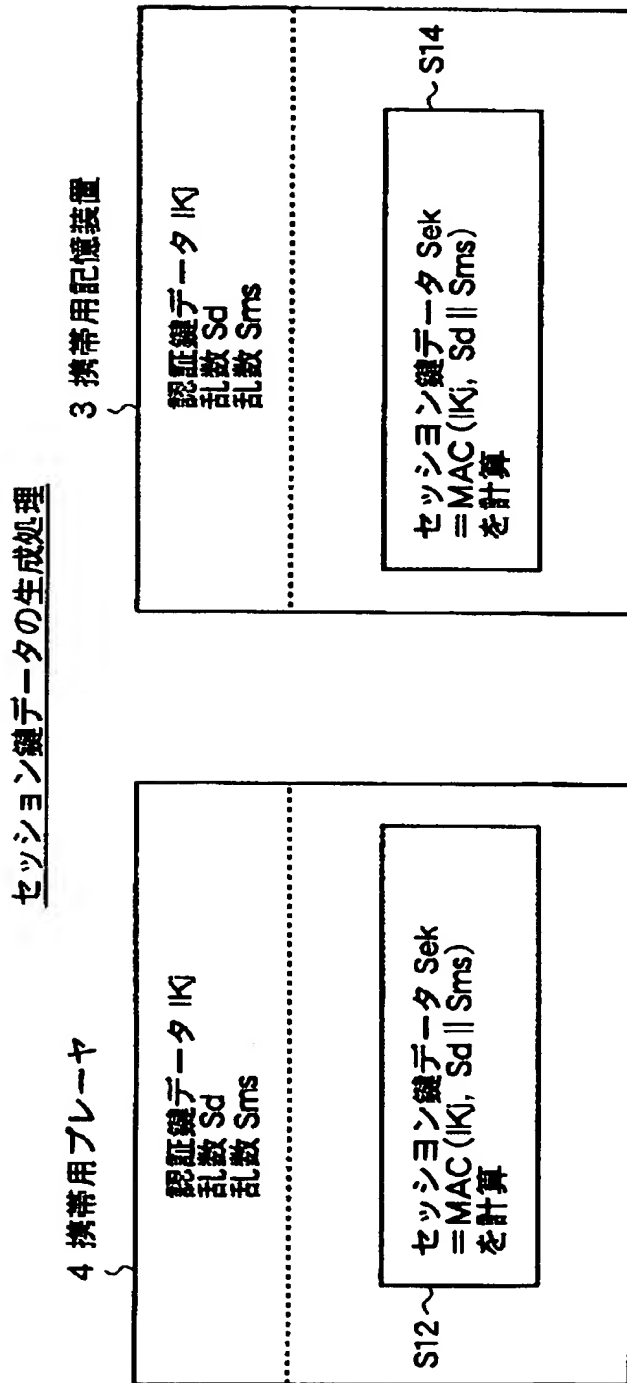
【图 13】



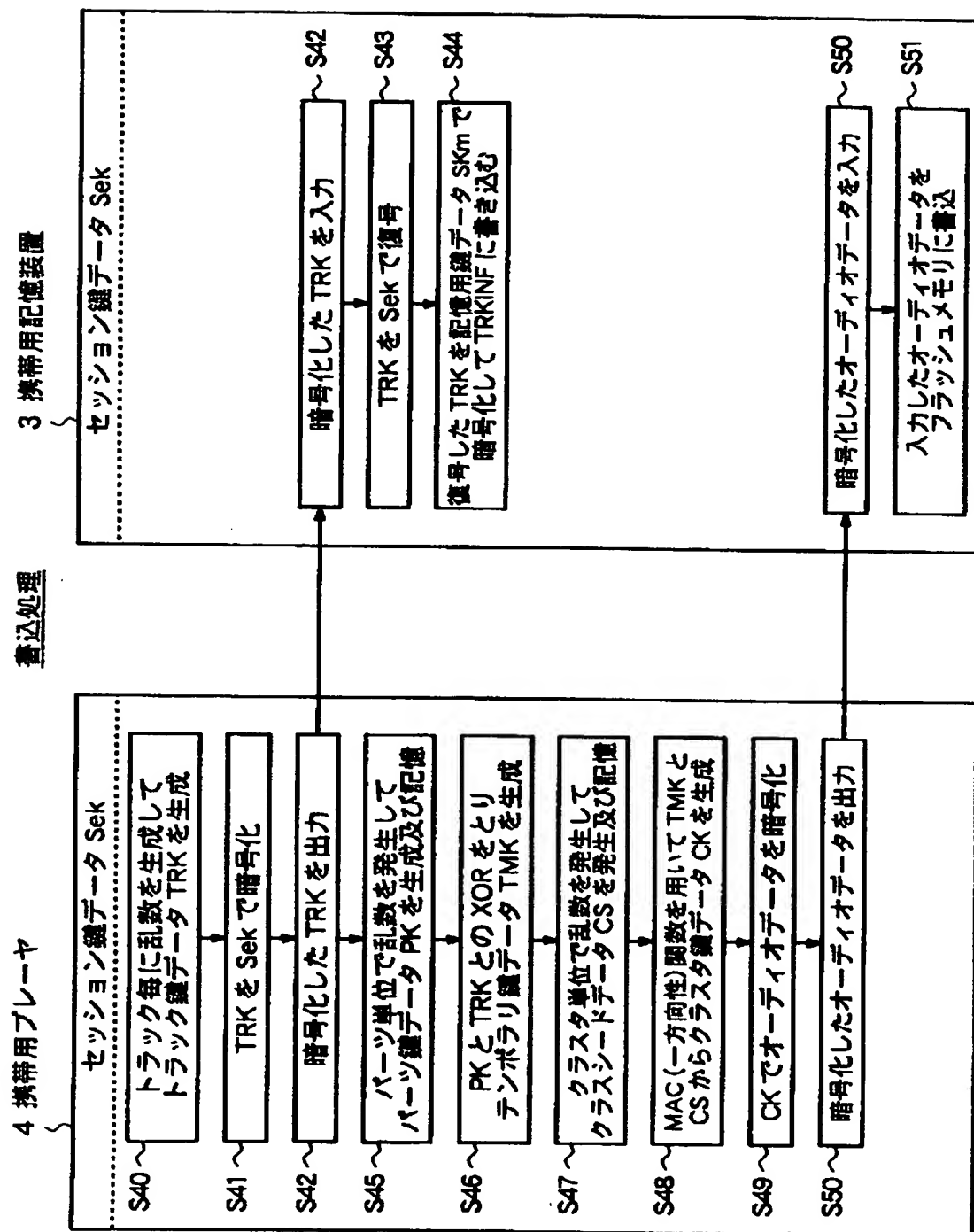
【図 1 4】



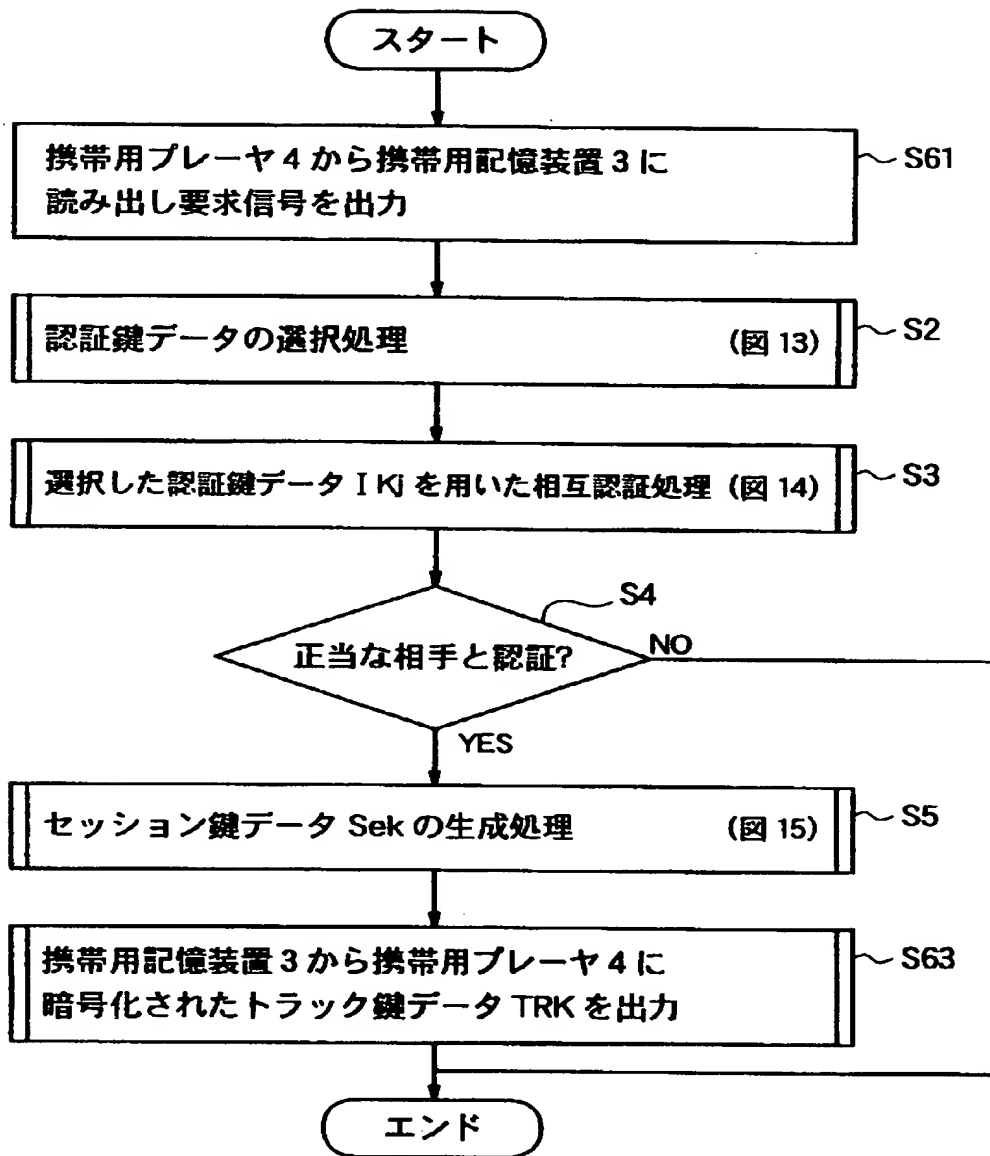
【図 1 5】



【図 16】

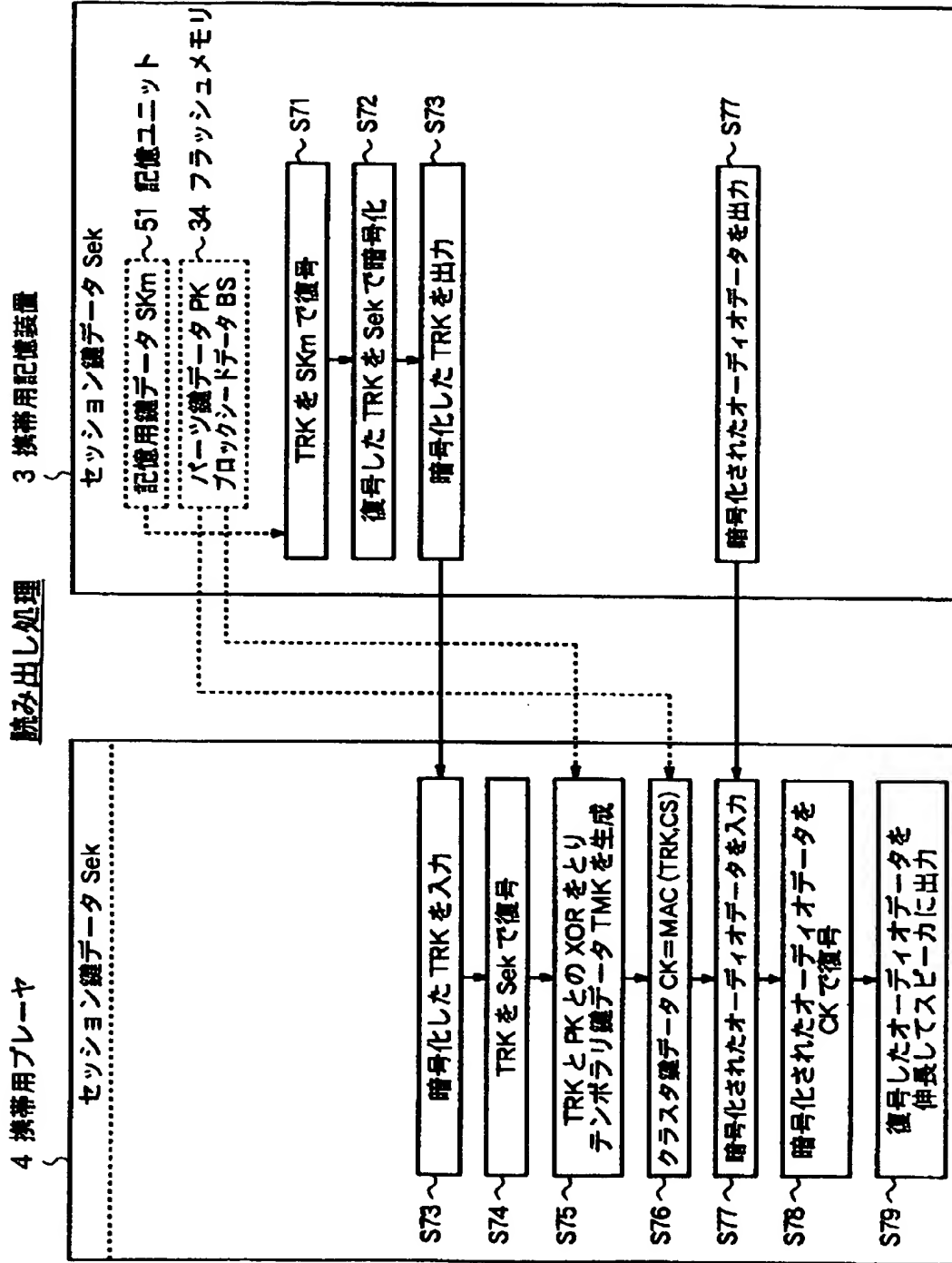


【図 17】

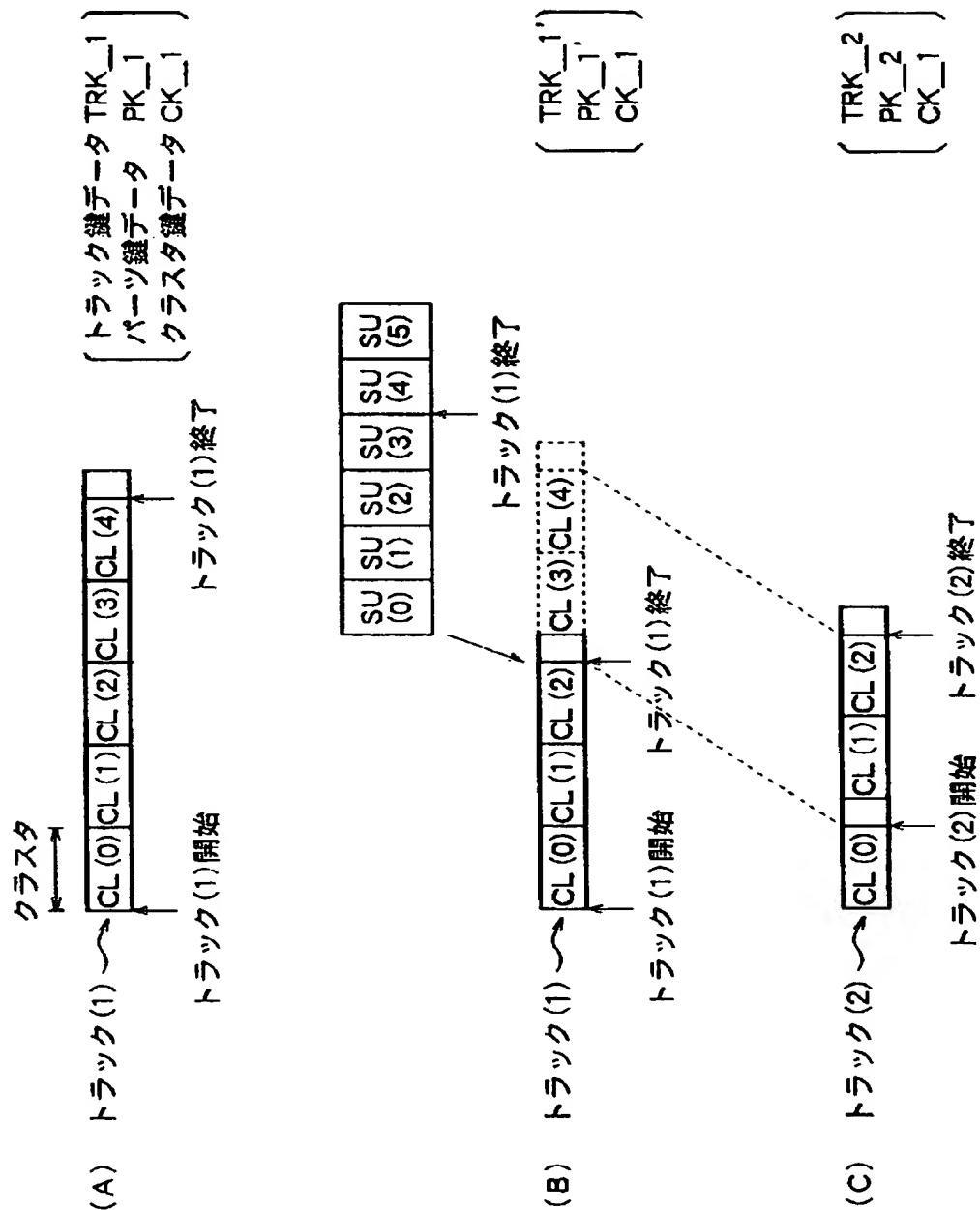


携帯用記憶装置 3 からの読み出し処理

【図 1 8】



【図 1 9】



トラック鍵データ TRK_1
パート鍵データ PK_1
クラスター鍵データ CK_1

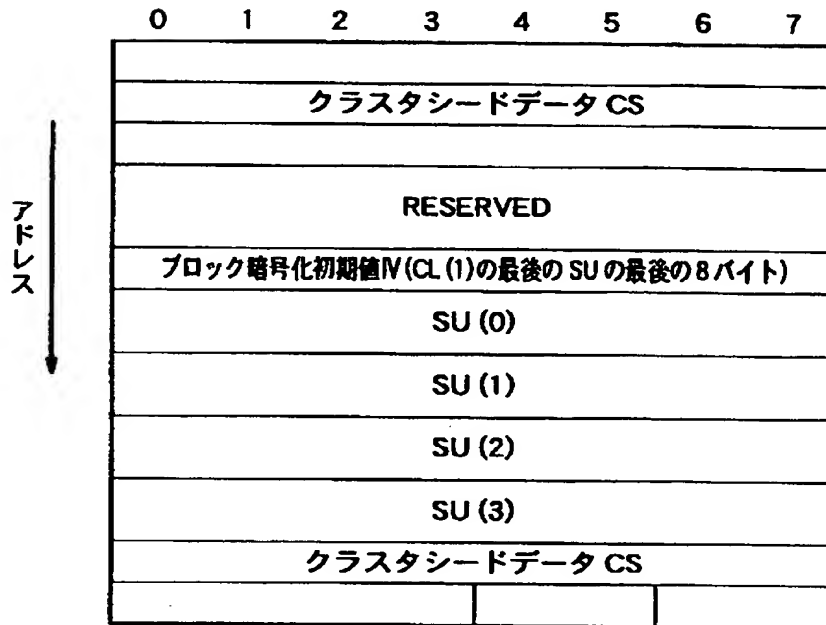
TRK_1'
PK_1'
CK_1'

TRK_2
PK_2
CK_1

【図 2 0】

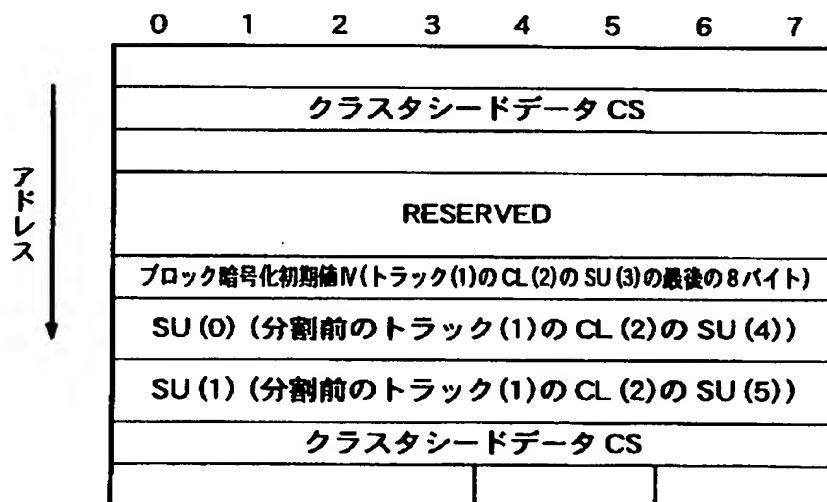
(A)

分割後のトラック(1)のクラスタ CL (2)

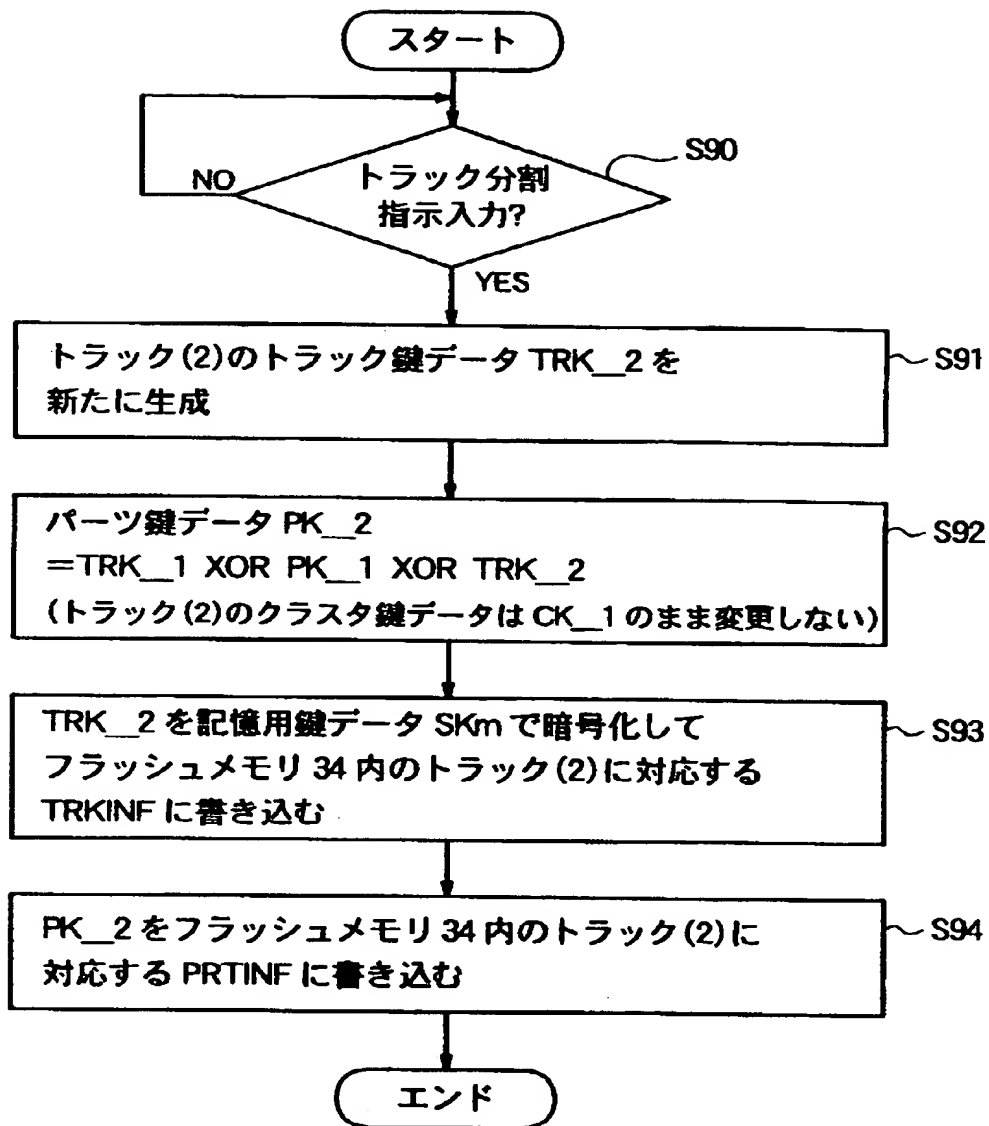


(B)

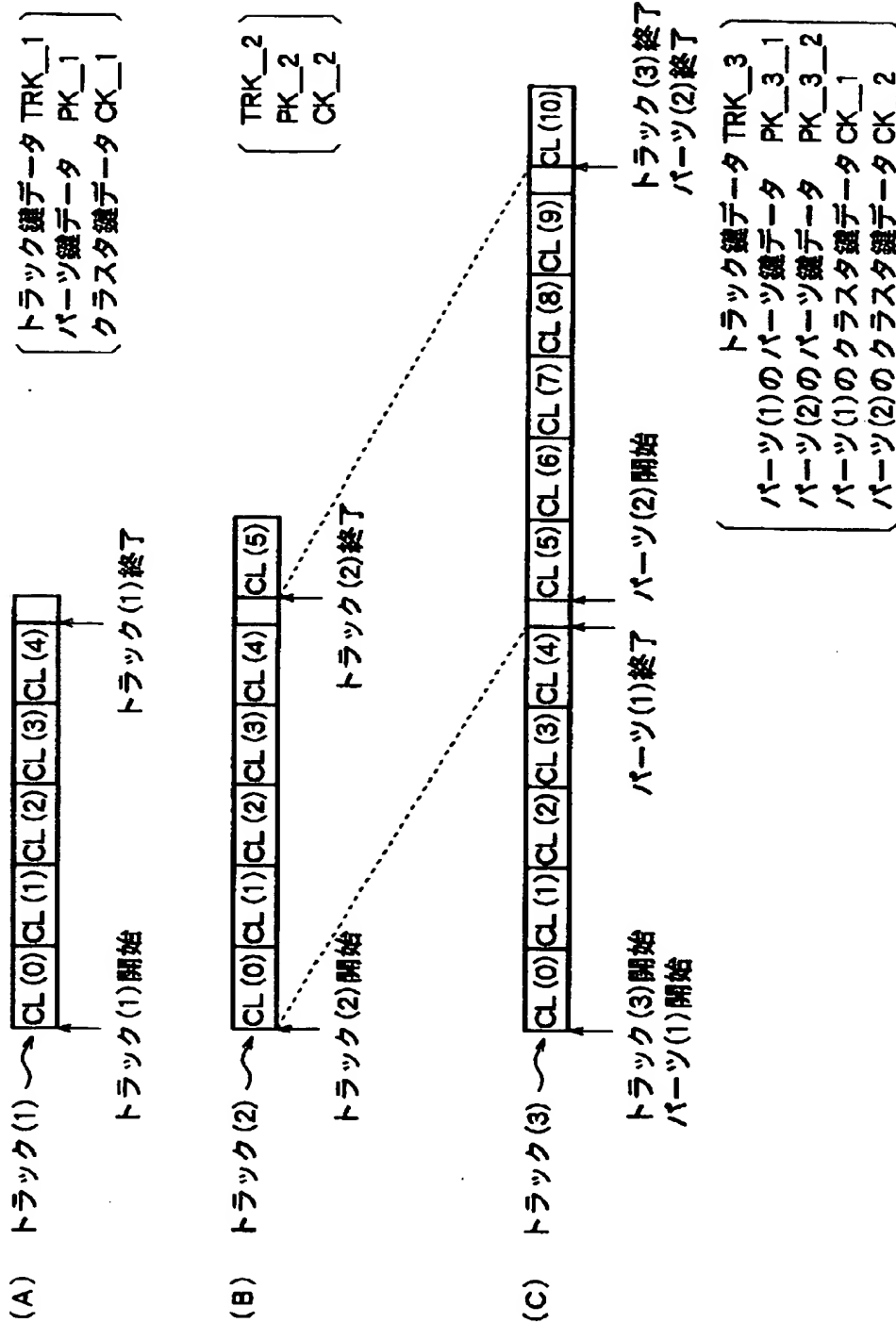
トラック(2)のクラスタ CL (0)



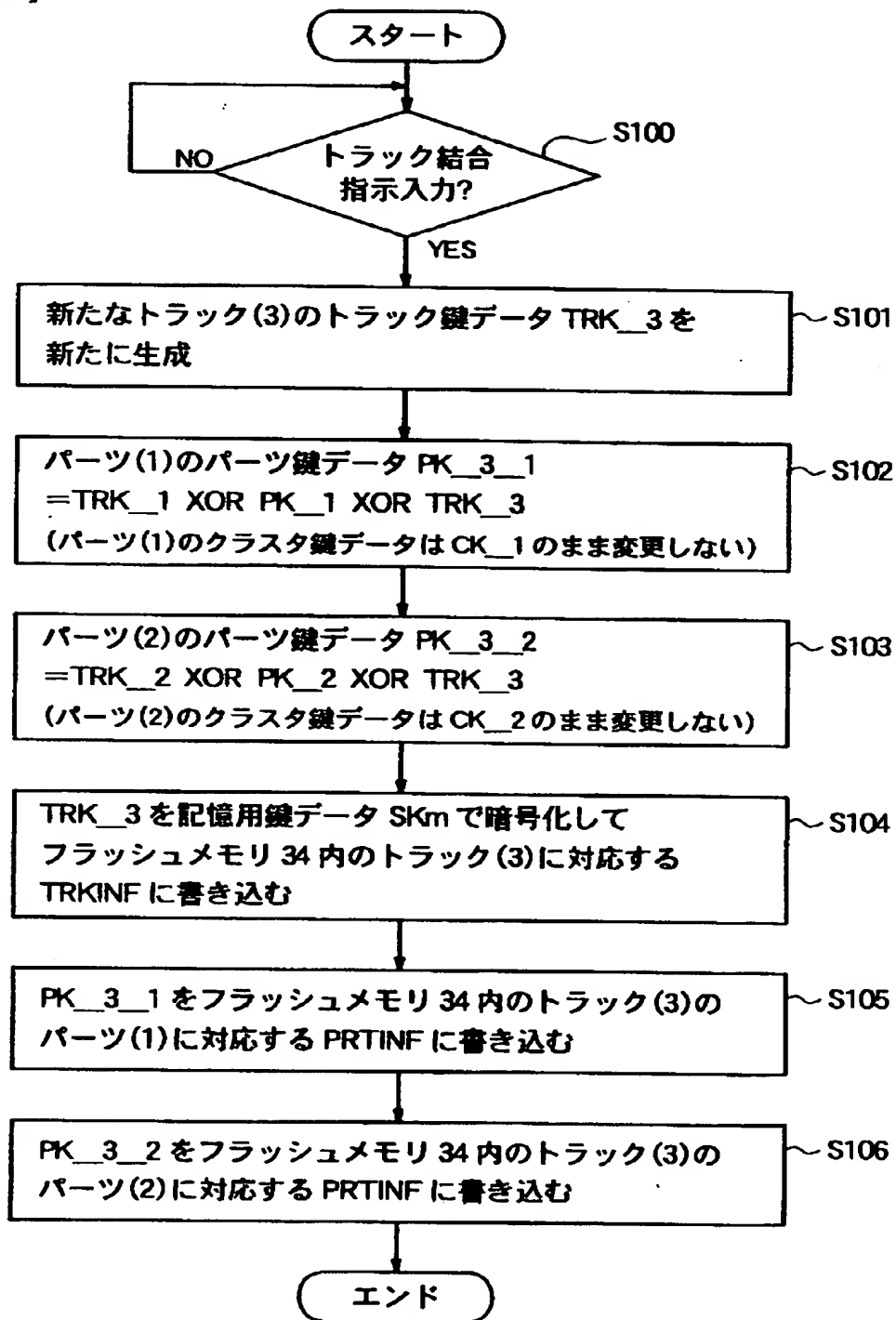
【図 21】



【図 2 2】



【図 2 3】



【書類名】 要約書

【要約】

【課題】 例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶媒体に記憶する際に、所定の処理ブロックに基づいた処理と復号処理とを簡単な構成で正確に行うことができるデータ処理装置を提供する。

【解決手段】 所定のデータ長の暗号化ブロックを単位としてデータを暗号化／復号ユニット 6 4 と、暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う圧縮／伸長モジュール 4 5 と、暗号化したデータを記憶するフラッシュメモリ 3 4 とを有し、携帯用プレーヤ 4 は、同じ暗号化ブロック内に位置するデータが同じ処理ブロック内に位置するように前記暗号化したデータをフラッシュメモリ 3 4 に書き込み、前記処理ブロックを単位として前記データをフラッシュメモリ 3 4 から読み出す。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社